Request for Proposals

Housing Voucher Processing Services

Issuance Date: March 22, 2024

Proposals must be submitted no later than 5:00 p.m. (EDT) on April 12, 2024

Submit to:
Ohio Housing Finance Agency
Janice Wildermuth, Purchasing Supervisor
FinRFP@ohiohome.org

Table of Contents

1. Guidelines for Request for Proposals

1.1 Introduction

The Ohio Housing Finance Agency (OHFA) is seeking proposals from qualified independent firms (Consultant) to perform monthly Housing Voucher Processing Services for the Ohio 811 Project Rental Assistance Program (Ohio 811 Program) and Ohio Department of Medicaid Subsidy Demonstration (ODMSD) Program. These programs provide the opportunity for individuals who are extremely low-income and have a disability to live in an integrated setting through rental subsidy and access to supportive services. Rental assistance covers the difference between 30 percent of the resident's income and the unit's 50 percent AMGI rent level calculated for the Ohio Low-Income Housing Tax Credit program.

Housing voucher processing services are being sought for the period of July 1, 2024 through June 30, 2028.

1.2 Timeline

OHFA has established the following schedule for selection of the housing voucher processing services provider:

Event	**Date**
RFP Issuance Date	Friday, March 22, 2024
Written questions from applicants	Friday, March 29, 2024 by 5:00 p.m. (EDT)
Responses to applicant questions	Friday, April 5, 2024 by 5:00 p.m. (EDT)
Proposals Due	Friday, April 12, 2024 by 5:00 p.m. (EDT)
Respondent Interviews, if required	Monday, April 22 – Thursday, April 25, 2024
Selection Confirmed by OHFA Board	Wednesday, May 15, 2024
Start Date of Services	Monday, July 1, 2024

The above schedule is subject to change upon notification on OHFA's website.

1.3 Submission of Written Questions

It is the policy of OHFA to accept questions and inquiries from all potential applicants. All questions and inquiries shall be in writing; no verbal inquiries will be honored. Potential applicants may submit their questions or inquiries via e-mail to: **FinRFP@ohiohome.org**. (Subject: Housing Voucher Processing Services RFP).

All emailed questions or inquiries are due by 5:00 p.m. (EDT) on Friday, March 29, 2024. OHFA expects to respond to all questions and inquiries by 5:00 p.m. (EDT) on Friday, April 5, 2024.

OHFA reserves the right to decline to respond to any question or inquiry that will cause an undue burden or expense for OHFA or which OHFA deems unnecessary for purposes of responding to this RFP. OHFA will post all questions or inquiries with answers on its website at **http://www.ohiohome.org**.

1.4 Verbal Communication Regarding RFP Prohibited

All communication from potential applicants regarding this RFP to OHFA staff and/or OHFA Board members is prohibited throughout the RFP process until the engagement is approved by the OHFA Board.

1.5 Submission of Proposals

Proposals received after the specified date and time will not be eligible for consideration. Any applicant who wishes to confirm receipt of their proposal may contact OHFA by E-mail to **FinRFP@ohiohome.org** (Subject: Housing Voucher Processing RFP Receipt Confirmation). OHFA will respond by e-mail with confirmation of receipt of the proposal.

An electronic copy of the written proposal must be sent to **FinRFP@ohiohome.org** (Subject: Housing Voucher Processing Services RFP) by 5:00 p.m. (EDT), Friday, April 12, 2024. This copy is to be submitted in portable document format (pdf). No paper submissions are needed, nor should they be submitted.

1.6 Right to Request Additional Information

OHFA reserves the right to request any additional information to assist in the review process.

1.7 Right to Reject Proposals and Cancel RFP

OHFA reserves the right to reject any and all proposals at any time. OHFA reserves the right to cancel, withdraw, modify or reissue this RFP at any time for any reason.

In connection with this RFP, OHFA reserves the right to waive any technicalities and make any award(s) that is determined to be in the Agency's best interests.

1.8 Evaluation and Award of Engagement

As described in Section 4, the RFP will be awarded to the firm that presents the most effective combination of qualifications, services, understanding of the specified Housing Voucher Processing Services, ability to identify and analyze key issues, experience with similar projects, quality of customer service, assurances and availability of key personnel, and cost.

1.9 Agreement for Services

The firm selected to provide the services described in this RFP is expected to sign the sample agreement (Exhibit B) for services covering the scope and terms of this RFP. Not agreeing to OHFA's terms may be a basis for rejection of selection or rejection of the response to this RFP. OHFA may require additional confidentiality and nondisclosure contract terms.

2. Scope of Services

2.1 Services Required

OHFA is seeking proposals from qualified independent firms to perform monthly housing voucher processing services for the Ohio 811 Program and ODMSD Program.

Ohio 811 Program

Rental Assistance Amount: Rental assistance covers the difference between 30 percent of the resident's income and the 50 percent Area Median Gross Income (AMGI) rent level calculated for the Low-Income Housing Tax Credit (LIHTC) program. The total rent cannot exceed the Fair Market Rent published by the U.S. Department of Housing and Urban Development (HUD).

HUD Vouchering: Vendor will receive HUD Form 50059 ("child voucher") and HUD 52670-A Part 2 Special Claims from participating property owners to the vendor's TRACS mailbox from owners' TRACS compliance software (e.g. Yardi, Bostonpost, OneSite, etc.). The vendor will verify that all information on the child voucher is correct and build HUD Form 52670 (the "parent voucher"), submitting the parent voucher to HUD contacts, and transmitting the voucher to TRACS.

Rental Assistance Contract Period: OHFA and the owners of participating properties enter into a 20-year Rental Assistance Contract (RAC). The Section 811 PRA funding guarantees rental assistance for the first five years, with the balance of the contract funded based on annual federal appropriations.

Units Served: OHFA currently has 471 Ohio 811 units in 73 developments under contract with approximately 370 units leased and reporting each month. The remaining units will be filled with 811 tenants as the current non-811 tenants move out of the units. OHFA has also begun identifying and committing 232 additional units to the program, which will be constructed and leased over the next four years.

Requested Services

a) Host a TRACS/iMAX mailbox ID to receive HUD Form 50059.
b) Review, edit, and certify HUD Forms 50059.
c) Roll up child vouchers into monthly parent voucher.
d) Use of the most current release of TRACS software.
e) Submit parent vouchers to HUD staff and TRACS.
f) Provide set-up assistance to new users.
g) Provide limited OHFA staff assistance as needed.

ODMSD Program

Description: The Ohio Department of Medicaid Subsidy Demonstration Program is a small-scale rental subsidy program administered by OHFA. The program was designed to replicate many aspects of the Ohio 811 Program. However, as a non-HUD program, the 26 monthly subsidy payments will need to be calculated and verified manually.

Rental Assistance Amount: Rental assistance covers the difference between 30 percent of the resident's income and the 50 percent AMGI rent level calculated for the LIHTC program. The total rent cannot exceed the Fair Market Rent published by HUD.

Rental Assistance Contract Period: OHFA and the owners of participating properties are in the fourth and fifth year of a 15-year contract.

Units served: OHFA currently serves 26 units in eight developments throughout the state through the ODMSD Program. No new units are anticipated.

Requested Services:

a) Tenant Certifications at move-in and annual recertifications.
b) Manual monthly Voucher Processing.
c) Monthly reporting to OHFA.
d) Provide set-up assistance to new users

2.2 Other Services

- Ongoing technical assistance to owners in submitting monthly rent reimbursement forms and correcting any identified errors.
- Ongoing technical assistance to OHFA staff as needed.

3. Proposal Requirements

3.1 Description of Firm

Describe the company and its experience performing Housing Voucher Processing Services. The description should include, but is not limited to, the following:

a) Location(s) and size.
b) If MBE/WBE/EDGE certified.
c) Number of years in operation.
d) Number of years' experience providing rental assistance payment processing services.
e) Experience providing rental assistance payment processing services for affordable housing clients.

3.2 Qualifications and Experience of Key Personnel

Designate the individual(s) who will be assigned to OHFA for this work. Provide a brief description of their relevant experience, expertise, and office location.

3.3 References

Provide a list of five client references for which your company has provided rental assistance payment processing services in the past five years. Include contact information for the client primary contact as well as a description of the services provided.

3.4 Methodology and Approach

Describe in detail how your organization proposes to satisfy each of the requirements of Section 2, Scope of Services. Indicate if any additional tasks are necessary and/or advisable.

3.5 Cost Proposal

Provide a detailed cost estimate for all components necessary to perform the services required in this RFP for the four-year contract period. The cost estimate must clearly state each of the following:

a) Startup Fee (if applicable).
b) Annualized Ongoing Maintenance Costs.
c) Annualized Per Unit or Per Project Costs.
d) Other Associated Annualized Costs.

See Exhibit A for a Cost Proposal Exhibit template.

3.6 Litigation, Administrative Proceedings, Investigations

Describe any pending or resolved material regulatory censure or litigation, regulatory action disclosure reporting, administrative proceedings, or investigations, in which your firm has been involved within the last three calendar years.

3.7 Security and Safety Rules

The selected Vendor must obtain an annual audit of the services being provided from the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAE) No. 18, Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2. The proposal must describe how these security and safety requirements will be satisfied. Describe ability for maintaining the security of information in accordance with the applicable security baseline of the current published version of the National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” (“NIST 800-53”) commensurate with the type of State Data involved in the Agreement in Exhibit B as communicated by the OHFA. Describe how you will comply with the Security and Safety Rules, as well as the Policies and Procedures provision contained in (Exhibit III to the Agreement contained in Exhibit B). Successful applicants will be processing confidential personal information of individuals receiving service under the federal programs. Lack of ability to meet security and safety rules may be grounds for disqualification.

4. Evaluation Process

4.1 Evaluation of Minimum Requirements

Each proposal will be evaluated to ensure that the applicant has complied with each section of this RFP and followed the formatting, organizational and submission requirements as described in this RFP.

4.2 Evaluation Criteria

In addition to the minimum requirements described above, the evaluation criteria will consist of a combination of the following:

- Section 2.1: Services Required
- Section 3.1: Description of Firm
- Section 3.2: Qualifications and Experience of Key Personnel
- Section 3.3: References
- Section 3.4: Methodology and Approach
- Section 3.5: Cost Proposal
- Section 3.6: Litigation, Administrative Proceedings, Investigations
- Section 3.7: Security and Safety Rules

If the respondent chosen by the evaluation team, based on all criteria other than cost, has a higher cost proposal than what OHFA determines as a reasonable cost, that respondent will be asked if it can provide the services for an amount OHFA determines to be reasonable. In considering which firm to select, OHFA has the right to negotiate the fee of any respondent that it believes will provide the best services at the most reasonable price that is in the best interests of and the most advantageous to the Agency. However, OHFA is not obligated to select the respondent with the lowest cost proposal.

The Executive Director of OHFA retains the ultimate discretion as to the awarding of this proposal to the firm they believe most meets the requirements in this proposal and is in the best interests of the Agency.

5. Submission Requirements

5.1 Organization and Format

OHFA requires the applicant to follow the formatting described below when submitting their proposal:

a) The electronic response must be submitted in portable document format (pdf).

b) Proposals will be organized and presented in order with the section headings and numbers listed below.

1. Each response to this RFP will include as the cover page a Letter of Transmittal. See Exhibit C for the format of the Letter of Transmittal.
2. Description of Firm
3. Qualifications and Experience of Key Personnel
4. References
5. Methodology and Approach
6. Cost Proposal
7. Litigation, Administrative Proceedings, Investigations
8. Security and Safety Rules

5.2 Submitting the Proposal

OHFA requires the applicant to submit one electronic copy of the proposal as explained in Section 1.5. By submitting a proposal, the applicant agrees to the following:

a) All materials submitted become the property of OHFA and shall be public information unless a statutory exception exists which would thereby determine that such information cannot be released to the public. If you have information in your proposal that you believe is an exemption to the public records laws you must identify each and every occurrence of the information in the proposal on a separate page titled “Exemptions to the Public Records Law”.

b) Applicants will respond to all requirements in this RFP and comply with any terms and conditions outlined in the RFP. Failure to do so may result in disqualification of the proposal.

c) All costs incurred in preparation of a proposal shall be borne by the applicant.

d) If during the evaluation process it becomes necessary to make further distinctions between certain applicants, OHFA may request certain applicants to make oral presentations of proposals to OHFA staff members, and/or an OHFA Evaluation Team.

e) Proposals received after the deadline will not be reviewed. Applicants are advised that there will be no opportunity to correct mistakes or deficiencies in their proposal after the submission deadline. Proposals that are missing required forms and or information may not be evaluated. It is the sole responsibility of the applicant to ensure its proposal is complete, accurate, responsive to the requirements, and received on time.

Exhibit A - Cost Proposal

Item	Description	Cost
Startup Fee **(if applicable)**		$
Annualized Ongoing Maintenance Costs		$
Annualized Per Unit or Per Project Costs		$
Other Associated Annualized Costs		$
	Total	**$**

Exhibit B – Agreement for Services

AGREEMENT FOR SERVICES

This Agreement for Services ("Agreement") is made and entered into by and between the **Ohio Housing Finance Agency**, (hereinafter referred to as "Sponsor" or "OHFA"), and _____ (hereinafter referred to as "Contractor"). Sponsor and Contractor may be collectively referred to in this Agreement as the "Parties".

STATEMENT OF THE AGREEMENT

NOW, THEREFORE, in consideration of the foregoing and the mutual promises and covenants hereinafter set forth, the parties agree as follows:

1. Statement of Work. Contractor will undertake and complete the work and activities set forth in the RFP and Contractor bid response, which are fully incorporated herein by reference as if fully rewritten, and as set forth in Exhibit I, "Scope of Work", attached hereto. Contractor will consult with Sponsor's personnel and with other appropriate persons, agencies, or instrumentalities as necessary to ensure a complete understanding of the work and satisfactory completion thereof. Contractor further warrants and represents that it has the necessary background, training, and skills to undertake and complete the work and activities set forth in Exhibit I and will do so through its best efforts. Best efforts is defined as being efforts performed in a workmanlike manner according to the highest professional standard for the purpose intended.

2. Sponsor's Instructions. Sponsor may, from time to time as it deems appropriate and necessary, communicate specific instructions and requests to Contractor concerning the performance of the work described in this Agreement. Upon notice and within a reasonable time, Contractor must comply with those specific instructions and fulfill those requests to Sponsor's satisfaction. It is expressly understood by the Parties that the instructions and requests are for the sole purpose of performing the specific tasks requested and to ensure satisfactory completion of the work described in this Agreement. Any specific instruments from the Sponsor under this provision are not intended to amend or alter the terms *o*f this Agreement or any part thereof. The management of the work, including the exclusive right to control or direct the manner or means by which the work described herein remains with and is retained by the Contractor. Sponsor retains the right to ensure that the work of the Contractor is in conformity with the terms and conditions of the Agreement, as specified in Exhibit I.

3. Term and Location of Performance.

a) Term. This Agreement is binding upon both parties, and the work described in this Agreement will commence on _____ and all activities under this Agreement will be completed not later than _____, on which date this Agreement will expire. In the event that the work hereunder is to be done in separate phases, each phase will be completed within the time prescribed in Exhibit I. In addition, if the Contractor and Sponsor desire to extend this Agreement for an additional period of time, an amendment will be executed setting forth the additional time period and an increase in the amount, as needed.

a) Location of Performance. Contractor affirms that it has read and understands Executive Order 2019-12D and 2022-02D issued by Ohio Governor DeWine, that it will abide by those requirements in the performance of this Agreement, and that it will perform no services required under this Agreement outside of the United States. The Executive Order is available at the following website:

https://governor.ohio.gov/wps/portal/gov/governor/media/executive-orders/2019-12d

https://governor.ohio.gov/media/executive-orders/executive-order-2022-02d

b) Change of Performance Location. Contractor also affirms, understands, and agrees to immediately notify Sponsor of any change or shift in the location(s) of services performed by Contractor or its subcontractors under this Agreement, and no services will be changed or shifted to a location(s) outside of the United States.

4. Compensation. In consideration of the mutual promises stated in this Agreement, Sponsor agrees to pay Contractor at the rates set forth in Exhibit I on a reimbursement basis upon Sponsor`s receipt and approval of proper invoices as more fully stated in section 5 of this Agreement. Section 126.30 of the Ohio Revised Code applies to this Agreement and requires payment of interest on overdue payments for all proper invoices. The interest charge shall be at a rate per calendar month which equals one-twelfth of the rate per annum prescribed by Section 5703.47 of the Ohio Revised Code. Contractor will not be compensated for services rendered except as expressly set forth herein. The total compensation to be paid to Contractor under this Agreement will not exceed _____ Thousand Dollars ($_____.00). Consequently, Contractor will only be paid for services actually performed which may be less than the total compensation allocated in this section. If travel expenses are contemplated and agreed upon by the Parties as necessary in order to perform the services described in Exhibit I, Contractor will be compensated for travel expenses at the rates set forth in the Office of Budget and Management's Travel Rules more fully stated in Ohio Administrative Code 126-1-02 (the "Expense Rule"). Contractor agrees that it will not be reimbursed and Sponsor will not pay any items that are deemed to be "non-reimbursable travel expenses" under the Expense Rule. This provision is subject to the compensation limit stated herein.

5. Proper Invoicing Method. Contractor must submit proper invoices that are itemized and clearly include all of the following:

a) Contractor's legal name, street address, email, phone number and (if applicable) fax number;
b) OHFA contact information including email address;
c) Invoice sent date and due date;
d) P.O. number or contract number;
e) Invoice number;
f) Terms of payment;
g) Delivery of the commodity or performance of the service described in Exhibit I;
h) Date or dates of the purchase or rendering of the service;
i) An itemization of the things or service done, the material supplied, respective hourly rate associated with the service performed or the amount of labor furnished; and
j) The sum due pursuant to that invoice in relation to the total compensation owed under the Agreement.

The adequacy and sufficiency of Contractor's invoices will be determined solely by Sponsor. If Sponsor determines that an invoice is inadequate or insufficient, or determines that further documentation or clarification is required for a particular invoice, the burden of providing the required information or documentation is on Contractor. Costs incurred by Contractor which are associated with providing the required additional information or documentation and costs related to defending an inadequate or insufficient invoice will not be charged to Sponsor and will not be considered an allowable expense under this Agreement. Failure to comply with this section will delay payment to Contractor under this Agreement. Further, a Purchase Order Number must be issued by the Sponsor prior to this Agreement being signed by the Sponsor.

6. Contractor's Expenses. Contractor is solely responsible for all office, business, and personal expenses associated with the performance of this Agreement unless otherwise stated herein.

7. Acknowledgment of Independent Contractor Status. Contractor acknowledges and agrees that any individual providing personal services under this Agreement is not a public employee for purposes of Ohio Revised Code ("ORC") Chapter 145. Sponsor considers Contractor to be an independent contractor or any other classification other than a public employee, and as such, will make no contributions to the public employees retirement system ("OPERS") on Contractor's behalf. If Contractor has fewer than five (5) employees, Contractor has been provided an acknowledgment form attached hereto as Exhibit II, which must be completed by the Contractor, returned to Sponsor, and subsequently sent to the Ohio Public Employees Retirement System within thirty (30) days of the start date of this Agreement as required under ORC Section 145.038. That acknowledgment form states that the individuals employed by the Contractor understand that they are independent contractors, not public employees, and as such are not entitled to OPERS benefits based on this Agreement. It is further agreed that neither Contractor nor its employees or agents are "employees" of Sponsor as the term is used in ORC Section 124.01(F) and, therefore, are not eligible for vacation, medical

insurance, sick leave, parental leave, leave of absence, tenure, bumping rights, retirement, or any other benefits or rights, which are incidents of public employment subject to the civil service laws of Ohio. Moreover, Contractor is responsible for any compliance with labor laws and contracts as it pertains to any union employees under its employment. Nothing herein contained will be construed to place the parties in the relationship of partners or joint venturers or of franchisor/franchisee.

8. Data and Information Control.

a) Confidentiality. The Contractor may learn of information, documents, data, records, or other material that is confidential in the performance of this Agreement. The Contractor may not disclose any information obtained by the Contractor as a result of this Agreement, without the Sponsor's written permission to do so. The Contractor must assume that all Sponsor information, documents, data, source codes, software, models, know-how, trade secrets, or other material is confidential. In addition, the Contractor may not disclose any documents or records excluded by Ohio law from public records disclosure requirements.

The Contractor's obligation to maintain the confidentiality of the information will not apply where the information:

i. Was already in the Contractor's possession before disclosure by the Sponsor, and the information was received by the Contractor without the obligation of confidence;

ii. Is independently developed by the Contractor;

iii. Is or becomes publicly available without breach of this Agreement except as provided in the next full paragraph;

iv. Is rightfully received by the Contractor from a third party without an obligation of confidence;

v. Is disclosed by the Contractor with the written consent of the Sponsor; or

vi. Is released in accordance with a valid order of a court or governmental agency, provided that the Contractor:

- Notifies the Sponsor of such order immediately upon receipt of the order; and

- Makes a reasonable effort to obtain a protective order from the issuing court or agency limiting disclosure and use of the confidential information solely for the purposes intended to be serviced by the original order of production.

Although some sensitive personal information, such as medical records, addresses, telephone numbers, and social security numbers may be publicly available through other sources, the Contractor will not disclose or use any sensitive personal information in any manner except as expressly authorized in this Agreement. Therefore, notwithstanding item iii above, the Contractor has an obligation to maintain the confidentiality of sensitive personal information and will do so.

The Contractor must return all original sources of information or data provided by the Sponsor and destroy any copies the Contractor has made on termination or expiration of this Agreement.

The Contractor will be liable for the disclosure of any confidential information. The Parties agree that the disclosure of confidential information originating from the Sponsor may cause the Sponsor irreparable damage for which remedies other than injunctive relief may be inadequate, and the Contractor agrees that in the event of a breach of the obligations hereunder, the Sponsor is entitled to temporary and permanent injunctive relief to enforce this provision without the necessity of proving actual damages. However, this provision will not diminish or alter any right to claim and recover damages.

Contractor will report security and privacy incidents to Sponsor in the most expedient time possible but not later than thirty days following its discovery or notification of the breach and will cooperate with the Sponsor and its response team in determining the scope of the breach and the affected users.

b) Public Records And Retention Of Documents And Information. The Contractor acknowledges that this Agreement, as well as any information, Deliverables (as such term is defined in Exhibit I), records, reports, and financial records related to this Agreement are presumptively deemed public records pursuant to ORC 149.43. The Contractor understands that these records must be made freely available to the public unless the Sponsor determines that, pursuant to state or federal law, the requested materials are confidential or otherwise exempt from disclosure. The Contractor must comply with any direction from the Sponsor to preserve or provide documents and information, in both electronic and paper form, and to suspend any scheduled destruction of such documents and information.

c) Security and Safety Rules. When using or possessing Sponsor data or accessing Sponsor networks and systems or acting as an agent of OHFA in administering a federal program, the Contractor, its employees, subcontractors and agents must comply with all applicable Sponsor

rules, policies, and regulations regarding Sponsor-provided IT resources, data security, and integrity. When on any property owned or controlled by the Sponsor, the Contractor must comply with all security and safety rules, regulations, and policies applicable to people on those premises.

The Contractor is responsible for maintaining the security of information in accordance with the applicable security baseline of the current published version of the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," ("NIST 800-53") commensurate with the type of State Data involved in the Agreement as communicated by the OHFA. If OHFA is providing the network layer, the Contractor must be responsible for maintaining the security of the information in environment elements that are accessed, utilized, developed, or managed by the Contractor. In either scenario, the Contractor must implement information security policies, standards, and capabilities as set forth in the Contract, adhere to OHFA's IT Security Policies and Standards, and use procedures in a manner that does not diminish established OHFA capabilities and standards. All work performed by the Contractor, all deliverables provided by the Contractor, and all environments utilized to perform the Contractor's work must comply with OHFA's IT Security Policies and Standards. The Contractor's information security and technology responsibilities with respect to the work and services the Contractor is providing to the OHFA include the following, where applicable:

i. Support OHFA IT security policies, standards and procedures development and maintenance activities. Assist in the implementation of associated security procedures with the OHFA's review and approval, including physical access requirements, User ID approval procedures, and a Security Incident action and response plan.

ii. Support implementation and compliance monitoring as per OHFA IT Security Policies and Standards.

iii. Upon identification of a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies.

The Contractor must obtain an annual audit of the services being provided under this Contract that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAE) No. 18, Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2. The audit must cover all operations pertaining to the services covered by this Agreement. The audit will be at the sole expense of the Contractor and the results must be provided to the Sponsor within 30 days of Contractor's receipt of its audit results each year.

The Sponsor may, at any time in its sole discretion, elect to perform a Security and Data Protection Audit. This includes a thorough review of Contractor controls, security and privacy functions and procedures, data storage and encryption methods, and backup and restoration processes. The Sponsor may utilize a third-party contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met. The Sponsor will provide its request in writing and will work with the Contractor to schedule time to conduct the audit.

At no cost to the Sponsor, the Contractor must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the services provided under this Agreement.

d). Cyber Liability Insurance Requirements. Cyber liability (first and third party) insurance with limits not less than $5,000,000 per claim and $5,000,000 aggregate shall be maintained by the Contractor. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in this Agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The coverage shall provide for breach response costs as well as regulatory fines and penalties and credit monitoring expenses with limits sufficient to respond to these obligations.

e). Policies and Procedures. Contractor shall be required to comply with all policies and procedures related to Sponsor's IT resources, data security and integrity as outlined in Exhibit III, which is attached hereto and made a part hereof.

9. Termination.

a) Termination for Convenience: The Sponsor may terminate this Agreement for its convenience by issuing written notice to the Contractor. The Contractor will be entitled to the pro-rated contract price for any Deliverable or portion of a Deliverable that the Contractor has delivered and the Sponsor has accepted before the written notice of termination. Total payments will not exceed the amount payable to the Contractor as if the Contract had been fully performed. Upon notice of termination, Contractor will immediately cease all work under this Agreement and take all necessary or appropriate steps to limit disbursements and minimize costs in ceasing all work. Contractor will be required to furnish a report setting forth the status of all activities under the Agreement including, but not limited to, the work completed and the payments received by Contractor and any other information as Sponsor may require. This will be the Contractor's exclusive remedy in the case of termination for convenience and is available to the Contractor only after the Contractor has submitted a proper invoice.

b) Termination for Breach. Sponsor may immediately terminate this Agreement, in

whole or in part, by written or oral notice to Contractor for any of the following reasons:

i. Contractor fails to perform the services or deliver the product further described in Exhibit I by the date required or by any later date as may be agreed upon by the Parties through an amendment to this Agreement;

ii. Sponsor determines that the services or product to be provided under this Agreement is inadequate for the initially intended use or cannot be feasibly adapted to the intended use;

iii. Any warranty or assurance provided by Contractor in this Agreement is found to have been false or incorrect when made or Contractor fails to immediately notify Sponsor that a warranty or assurance in this Agreement was subsequently found to be false or incorrect;

iv. Contractor or any of its subcontractors perform services under this Agreement outside the United States;

v. Contractor makes any general assignment for the benefit or creditors, closes its business, becomes subject to a court order appointing a receiver, trustee, or similar official to act on its behalf, or files bankruptcy;

vi. Contractor becomes the subject of any proceeding under any law related to bankruptcy, insolvency, reorganization, or relief from debtors; or

vii. In Sponsor's sole opinion, Contractor becomes insolvent or in an unsound financial condition so as to endanger performance under this Agreement.

The Sponsor, in its sole discretion, may provide written notice to Contractor of a breach and permit the Contractor to cure the breach. The cure period provided by Sponsor may not exceed 21 calendar days. During the cure period, the Sponsor may buy substitute services from a third party and recover from the Contractor any costs associated with acquiring those substitute services. Notwithstanding the Sponsor permitting a period of time to cure the breach or the Contractor's cure of the breach, the Sponsor does not waive any of its rights and remedies provided the Sponsor in this Agreement, including but not limited to recovery of funds paid for services the Contractor performed outside of the United States, costs associated with corrective action, or liquidated damages.

Sponsor will not be obligated to pay for any services or products provided under this Agreement if Contractor's actions result in any one of the conditions for Termination for Breach described above. Contractor will also immediately return all funds paid to the Sponsor if it or any of its

subcontractors cause a Termination for Breach to occur. Sponsor may also recover all costs associated with any corrective action that it may undertake from the Contractor if the Contractor or any of its subcontractors cause a Termination for Breach to occur, including an audit or risk analysis related to Contractor's performance of services outside the United States. The Sponsor may also recover all accounting, administrative, legal and other expenses reasonably necessary for the preparation of the termination of the Agreement and costs associated with the acquisition of substitute services from a third party.

c) Termination for Just Cause. Sponsor may terminate this Agreement, in whole or in part, for just cause upon thirty (30) days written notice to the Contractor. Upon notice of termination, Contractor will immediately cease all work under this Agreement and take all necessary or appropriate steps to limit disbursements and minimize costs in ceasing all work. Contractor will be required to furnish a report setting forth the status of all activities under the Agreement including, but not limited to, the work completed and the payments received by Contractor and any other information as Sponsor may require. Subject to any claim for damages arising from Contractor's breach, Contractor will be entitled to compensation for work completed through the date Contractor received notice of termination upon submission and approval of proper documentation or invoices.

d) Waiver. No term or provision of this Agreement will be deemed waived and no breach excused unless the waiver of consent is in writing and signed by both Parties to this Agreement.

e) Costs Associated with Termination for Cause.

i. Sponsor may recover all accounting, administrative, legal and other expenses reasonably necessary for the preparation of the termination of the Agreement and costs associated with the acquisition of substitute services from a third party.

ii. If the Sponsor determines that actual and direct damages are uncertain or difficult to ascertain, the Sponsor in its sole discretion may recover a payment of liquidated damages in the amount of one percent of the value of the Agreement.

10. Certification of Funds. It is expressly understood by Sponsor that none of the rights, duties, and obligations described in this Agreement will be binding on either party until all statutory provisions under the Ohio Revised Code and procedural requirements under OHFA's bylaws have been complied with. Moreover, no act by OHFA's Board is considered binding upon or a restriction upon a future OHFA Board. If at any time sufficient funds are not available or appropriated to continue funding any payment due under this Agreement, this Agreement will terminate in accordance with the "Termination for Just Cause" provision in Article 9(c).

11. Equal Employment Opportunity. Pursuant to ORC 125.111, Contractor agrees that Contractor, any subcontractor, and any person acting on behalf of Contractor or subcontractor, will not discriminate, by reason of race, color, religion, sex, age, disability, national origin, military status or ancestry against any citizen of this state in the employment of any person qualified and available to perform the work under this Agreement. Contractor further agrees that Contractor, any subcontractor and any person acting on behalf of Contractor or subcontractor will not, in any manner, discriminate against, intimidate, or retaliate against any employee hired for the performance of work under this Agreement on account of race, color, religion, sex, age, disability, national origin, military status or ancestry. Contractor represents that it has a written affirmative action program for the employment and effective utilization of disadvantaged persons and will file a description of that program and a progress report on its implementation with the equal employment opportunity office of the department of administrative services. Contractor and any of its subcontractors are encouraged to use MBE and EDGE vendors to assist in completing the work under this Agreement.

12. No Unfair Labor Practice Findings. Contractor warrants and represents that neither it nor any or its subcontractors are listed with the Secretary of State for unfair labor practices, pursuant to ORC 121.23.

13. Forbearance. No act of forbearance or failure to insist on the prompt performance by Contractor of its obligations under this Agreement, either express or implied, will be construed as a waiver by Sponsor of any of its rights hereunder.

14. Indemnification. The Contractor agrees to indemnify and to hold the Sponsor and State of Ohio harmless and immune from any and all claims for injury or damages arising from this Agreement and the Contractor's performance of the obligations or activities in furtherance of the Agreement which are attributable to the Contractor's own actions or omissions or those of its trustees, officers, employees, subcontractors, suppliers, third parties utilized by the Contractor, or joint venturers while acting under this Agreement. Claims that the Contractor will indemnify the Sponsor and State of Ohio include, but are not limited to, any claims made under the Fair Labor Standards Act or under any other federal or state law involving wages, overtime, or employment matters and any claims involving patents, copyrights, and trademarks. The Contractor will bear all costs associated with defending the Sponsor and the State of Ohio against any claims.

15. Ohio Ethics Laws. Contractor, by its signature on this document, certifies: (1) it has reviewed and understands the Ohio ethics and conflict of interest laws including, without limitation, ORC 102.01 *et seq*., 2921.01, 2921.42, 2921.421, 2921.43, and 3517.13(I) and (J); and (2) it has not taken and will not take any action inconsistent with those laws, as any of them may be amended or supplemented from time to time.

15. Drug-Free Workplace Compliance. In the event that work performed pursuant to the terms of this Agreement will be done while on state property, Contractor hereby certifies that all

of its employees, while working on state property, will not purchase, transfer, use or possess illegal drugs or alcohol or abuse prescription drugs in any way.

16. Adherence to State and Federal Laws, Regulations. Contractor agrees to comply with all applicable federal, state, and local laws in the conduct of the work under this Agreement. Contractor and its employees are not employees of Sponsor with regard to the application of the Fair Labor Standards Act minimum wage and overtime payments, Federal Insurance Contribution Act, the Social Security Act, the Federal Unemployment Tax Act, the provisions of the Internal Revenue Code and for state revenue and tax laws, state workers' compensation laws and state unemployment insurance laws. Contractor accepts full responsibility for payment of all taxes including, with limitation, unemployment compensation insurance premiums, all income tax deduction, social security deductions, and any and all other taxes or payroll deductions required for all employees engaged by Contractor in the performance of the work authorized by this Agreement. Contractor is solely responsible for obtaining its own workers' compensation coverage for itself and its employees. Sponsor is exempt from federal, state and local taxes and will not be liable for any taxes under this Agreement.

17. Unresolved Findings. Contractor warrants that it is not subject to an unresolved finding for recovery under O.R.C. 9.24. If this warranty is deemed to be false, this Agreement is void *ab initio* and the Contractor must immediately repay to the Sponsor any funds paid under this Agreement. Contractor further warrants that it has no outstanding final judgments against it by the State, including tax liabilities, and agrees that any payments incurred by the State in this Agreement may be applied against any outstanding judgments or liabilities currently owed to the State or incurred by the State in the future.

18. Conflict of Interest. Contractor certifies that it does not have on its staff, payroll, or otherwise employed for monetary compensation or not, any employee who, within the past twelve months, was a public official or employee with Sponsor or any other board, commission or agency of the State of Ohio who had the ability to make decisions regarding approval, disapproval, recommendation, rendering advice, investigation or otherwise exercised substantial administrative control over matters concerning Contractor at the time of his or her state employment. Further, no personnel of Contractor, subcontractor of Contractor or personnel of any such subcontractor, or public official who exercises any functions or responsibilities in connection with the review or approval of any work completed under this Agreement will, prior to the completion of such work, voluntarily or involuntarily acquire any personal interest, direct or indirect, which is incompatible or in conflict with the discharge or fulfillment of his functions or responsibilities with respect to the completion of the work contemplated under this Agreement. Any such person, who, prior to or after the execution of this Agreement, acquires any personal interest, involuntarily or voluntarily, must immediately disclose his interest to Sponsor in writing. Thereafter, the affected person will not participate in any action affecting the work under this Agreement unless Sponsor determines that, in light of the personal interest disclosed, their participation in that action would not be contrary to the public interest.

20. Force Majeure (Excusable Delay). As used in this Agreement, the term "force majeure" includes all events that cause delay in the performance under that Agreement due to events or causes beyond its or its subcontractor's control and without its or its subcontractor's negligence or fault. For purposes of this section, the term "force majeure event" includes without limitation, the following: (1) Acts of God, such as epidemics, pestilence, lightning, earthquakes, fires, storms, hurricanes, tornadoes, floods, washouts, droughts, or other severe weather disturbances; (2) other events or causes that could not be foreseen in the exercise of ordinary care and beyond the reasonable control of the affected party, such as explosions, restraining of government and people, war, strikes, and other similar events or causes.

If the Sponsor or the Contractor cannot perform any part of its obligations under this Agreement because of force majeure, that party is excused from those obligations, to the extent that performance is prevented by the force majeure event and that party took all commercially reasonable steps to mitigate or avoid the effects of the force majeure event. If there is only a delay in performance, such delay may extend only for that time lost because of the force majeure event. At any time a party is unable to perform those above-referenced obligations, it must also do the following:

a) Promptly notify the other party, in writing, of any material delay in performance due to a specified force majeure event;

b) Provide detailed information of the force majeure event;

c) Provide a proposed revised performance date to make up for performance delays due to the force majeure event. When applicable, the revised schedule must provide for performance time not to exceed the time lost as a result of the force majeure event.

21. Prohibition Of The Expenditure Of Public Funds For Offshore Services. No State Cabinet Agency, Board or Commission will enter into any contract to purchase services provided outside of the United States or that allows State Data to be sent, taken, accessed, tested, maintained, backed-up, stored, or made available remotely outside (located) of the United States, unless a duly signed waiver from the State has been attained. Notwithstanding any other terms of this Agreement , the Sponsor reserves the right to recover any funds paid for services the Contractor performs outside of the United States for which it did not receive a waiver. The Sponsor does not waive any other rights and remedies provided to the Sponsor in the Agreement.

Further, no State agency, board, commission, State educational institution, or pension fund will make any purchase from or investment in any Russian institution or company. Notwithstanding any other terms of this Agreement, the Sponsor reserves the right to recover any funds paid to Contractor for purchases or investments in a Russian institution or company in violation of this paragraph. The provisions of this paragraph will expire when the applicable Executive Order is no longer effective.

The Contractor must complete the Contractor/Subcontractor Affirmation and

Disclosure Form affirming the Contractor understands and will meet the requirements of the above prohibition. During the performance of this Contract, if the Contractor changes the location(s) disclosed on the Affirmation and Disclosure Form, Contractor must complete and submit a revised Affirmation and Disclosure Form reflecting such changes.

State Data shall mean the following: All data and information provided by, created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data. Sensitive Data means any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted or disclosed without authorization. Sensitive Data includes, but is not limited to:

a) Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers;
b) Federal Tax Information (FTI) under IRS Publication 1075;
c) Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA);
d) Criminal Justice Information (CJI) under the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy and the Law Enforcement Automated Data System (LEADS) Policy; and
e) Other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

21. Miscellaneous.

a) Governing Law. This Agreement is governed by the laws of the State of Ohio as to all matters, including any challenge to its validity, enforceability, construction, effect, and performance.

b) Forum and Venue. All actions regarding this Agreement will be forumed and venued in a court of competent subject matter jurisdiction in Franklin County, Ohio.

c) Entire Agreement. This Agreement and its exhibits and any documents referred to herein, including the RFP and Scope of Work, constitute the complete understanding of the Parties and merge and supersede any and all other discussions, agreements and understandings, either oral or written, between the parties with respect to the subject matter hereof.

d) Severability. Whenever possible, each provision of this Agreement is to be interpreted in such a manner as to be effective and valid under applicable law, but if any provision of this Agreement is held to be prohibited by or invalid under applicable law, that provision will be ineffective only to the extent of that prohibition or invalidity finding, without invalidating the remainder of such provisions of this Agreement.

e) Notices. All notices, consents, demands, requests and other communications which may or are required to be given hereunder must be in writing and will be deemed duly given if personally delivered or sent by United States mail, registered or certified, return receipt requested, postage prepaid, to the addresses set forth below or to another address designated by the applicable party in written notice transmitted in accordance with this provision.

In case of Sponsor, to:

Ohio Housing Finance Agency
2600 Corporate Exchange Dr., Suite 300
Columbus, Ohio 43231

In case of Contractor, to:

_____

_____

_____

f) Amendments or Modifications. Either Party may at any time during the term of this Agreement request amendments or modifications. Requests for an amendment or modification of this Agreement must be in writing and specify the requested changes and the justification for those changes. Should the Parties consent to an amendment to or modification of the Agreement, then an amendment will be drafted, approved, and executed in the same manner as the original agreement. Any amendment or modification to the Agreement must be in writing and signed by both Parties to be effective.

g) Pronouns. The use of any gender pronoun includes all the other genders, and the use of any singular noun or verb includes the plural, and vice versa, whenever the context so requires.

h) Headings. Section headings contained in this Agreement are inserted for convenience only and are not considered a part of this Agreement.

i) Assignment. Neither this Agreement nor any rights, duties, or obligations described herein may be assigned or subcontracted by Contractor without the Sponsor's prior express written consent. Any assignment or delegation without the Sponsor's prior express consent, is voidable by the Sponsor.

j) Refrainment from Boycott. Pursuant to ORC 9.76, Contractor agrees that it will

refrain from boycotting any jurisdiction with whom the State can enjoy open trade, including Israel, during the contract period.

k) Electronic Signatures. Copies of signatures sent by facsimile transmission or provided electronically in portable document format ("PDF") are deemed to be originals for purposes of execution and proof of this Agreement.

l) Taxes: Sponsor is exempt from federal excise taxes and all state and local taxes, unless otherwise provided herein.

IN WITNESS WHEREOF, the parties have executed this Agreement for Services on the last day and year set forth below.

Contractor	State of Ohio
INSERT NAME:	Ohio Housing Finance Agency:
_____	_____
	Executive Director
Title: _____	
Date:_____	Date: _____

Exhibit C – Letter of Transmittal

Note: Submit the following on your firm's letterhead

Letter of Transmittal

Ohio Housing Finance Agency
Attn: Janice Wildermuth, Purchasing Supervisor
Housing Voucher Processing Services – RFP Request
2600 Corporate Exchange Dr., Suite 300
Columbus, Ohio 43231

Dear Ohio Housing Finance Agency:

In accordance with the Request for Proposal, we are pleased to submit our written proposal.

_____ (insert firm's name) will provide housing voucher processing services to OHFA for the period of July 1, 2024 to June 30, 2028 in accordance with the requirements of the Request for Proposal issued by OHFA.

Any information or questions concerning this written proposal should be directed to _____ (firm's liaison) at the following email address and telephone number: _____.

Respectfully,

_____ (signature)
Authorized Officer of Firm
Printed Name and Title
Email Address
Phone Number

OHIO HOUSING FINANCE AGENCY

Exhibit D

POLICIES AND PROCEDURES APPLICABLE TO ALL OHFA IT CONTRACTORS

All IT contractors are required to comply with all of the policies and procedures set forth in this Exhibit III.

INDEX FOR POLICIES AND PROCEDURES FOR IT CONTRACTORS

POLICY ON PROTECTING PRIVACY (C6)

I. PURPOSE

OHFA takes seriously the protection of Personally Identifiable Information and Confidential Personal Information. This policy provides the requirements for protecting the privacy of people and businesses who have information in our databases, electronic and paper files and other records. This policy lays out basic handling expectations for all types of Personally Identifiable Information and it provides important additional handling requirements for Confidential Personal Information.

II. RELATED LAWS, RULES, POLICIES, REQUIREMENTS OR STANDARDS

- ORC 1347.01 – Personal Information Systems Definitions
- ORC 1347.15 – Access Rules for Personal Confidential Information
- OAC 175-10 – Accessing Confidential Personal Information
- Clean Desk Policy F18
- Use of Internet, E-mail and Other IT Resources C7
- Data Encryption and Securing Sensitive Data C8
- Public Records Request Policy D5
- Sensitive Paper Document Handling Policy D6
- Records Management F10
- Accessing and Logging Confidential Personal Information in a Computer-based System Procedure (system specific)
- Accessing Confidential Personal Information in a Paper-based System Procedure (system specific)
- Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure
- Request to Inspect Personal Information Procedure

III. APPLICABILITY

This policy applies to all OHFA employees, temporary personnel, contractors and others who gain access to the OHFA physical facility, state e-mail system and/or Agency-supplied internet and network services.

IV. DEFINITIONS

Confidential Personal Information (CPI) – PII that falls within the scope of section 1347.15 of the Revised Code and that OHFA is prohibited from releasing under Ohio's public records law.

De-identification – A general term for any process of removing the association between a set of identifying data and the data subject.

Personally Identifiable Information (PII) - For the purposes of this policy, "PII" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person, and
- any information that indicates that a person possesses certain personal characteristics.

Removable Media - Any portable device that is capable of storing information. Media is not required to be capable of processing information.

This definition includes, but is not limited to, the following:

- Diskettes
- External/removable hard drives
- Flash memory (e.g., secure digital (SD), Compact Flash, secure digital high capacity (SDHC), solid state drives, memory sticks)
- Magnetic tapes
- Portable Devices
- Optical media such as compact disks (CDs), digital video disks (DVDs), etc.
- Thumb drives (USB keys)/jump drives

Sensitive Data - Sensitive Data is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. The data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

V. POLICY

OHFA employees, temporary personnel, contractors and others as outlined above, must abide by the OHFA policies and related laws, rules, policies and standards listed in Section II; and abide by the following procedures on handling all information whenever they know or have reason to believe that the information contains PII, CPI or other Sensitive Data.

VI. PROCEDURES

PII falling into the wrong hands can lead to identity theft. The following procedures help to ensure PII remains secure.

A. Handling All PII

- Use PII only for official, operationally necessary and lawful purposes.
- Do not access systems with PII – whether electronic or paper – if you have not been authorized to do so. Contact your supervisor if you need access.
- Enter PII accurately. Make a good faith effort to correctly enter data. Never intentionally enter false data.
- Apply De-identification techniques wherever possible, to transmit or receive any PII or CPI through a secure server and to encrypt emails that contain any sensitive information. (See section IX. ATTACHMENTS and Data Encryption and Securing Sensitive Data C8)
- Take reasonable precautions to protect PII from unauthorized modification, destruction, use or disclosure. Whenever an individual requests information that OHFA maintains about that individual, OHFA employees, temporary personnel and contractors shall follow OHFA's Request to Inspect Personally Identifiable Information Procedure.
- You always have a duty not to disclose PII without proper agency authorization. As you do your work, you may inadvertently or unintentionally come in contact with information that you know or have reason to believe is PII. In those circumstances, you have a duty not to disclose that PII to anyone except properly authorized persons.
- Only collect PII when you have been authorized to do so by the proper OHFA manager as part of your work responsibilities. Do not create an electronic or paper system of record with PII unless you have OHFA authorization and follow OHFA-mandated privacy and security requirements.
- Secure Sensitive Data in Transmission: The following methods shall be employed to secure Sensitive Data transmission:
    - Email: Sensitive Data transmitted through email must be encrypted by using Zix™ in the Outlook client or setting the email sensitivity to "Confidential." See also section IX.
    - Secure FTP: FTP clients employed for the transmission of Sensitive Data must use a Secure Shell or SSH network protocol to exchange the data over a secure channel.
    - Secure Web Sites: Sensitive Data may only be downloaded from or uploaded to websites with HTTPS encryption and user authentication.
    - Removable Media: Use of Removable Media to store Sensitive Data is prohibited. Sensitive Data placed on media by external partners and sent to OHFA must be encrypted.
- Destroy PII securely in accordance with corresponding record retention schedules (See Records Management F10) and follow OHFA data destruction procedures for particular systems or records (See Sensitive Paper Document Handling Policy D6)
- Do not initiate or otherwise contribute to any disciplinary or other punitive action against any individual who reports evidence of unauthorized use of PII.
- OHFA monitors its information, systems, other IT assets, employees and contractors for compliance with this policy. Therefore, employees and contractors have no expectation of privacy when they use state information, systems and IT assets.

B. Because CPI requires a higher standard of care, employees accessing the following CPI systems shall follow the privacy procedure specific to that system:

See Access and Logging Confidential Personal Information in a Computer-Based System Procedures for the following systems:

- DevCo
- DocuWare
- Finance Systems
- Hardest Hit Fund – Allita 360
- Multifamily Program Compliance – Allita 360
- Residential Lending Division – Homebuyer Program System

See Accessing Confidential Personal Information in a Paper-based System for:

- Human Resource Employee and Applicant Records

Nothing in this policy restricts the release of public records. PII and CPI is only confidential if Ohio law prohibits the agency from its release. (See the Public Records Request Policy D5 for guidance on this issue).

VII. COMPLIANCE

- Any employee who violates this policy is subject to the Discipline Policy A-35 and the OCSEA Bargaining Unit Contract as appropriate.
- Any employee who violates a confidentiality statute or OAC Chapter 175-10 is subject to criminal charges, civil liability arising out of the employee's actions, employment termination and a lifelong prohibition against working for the State of Ohio.
- Any violation of this policy by a contractor may be considered a material breach of the contract and may subject the contract to termination. Any contractor who violates a confidentiality statute may also be subject to criminal charges and civil liability arising out of the contractor's actions. The vendor may also be subject to vendor debarment.
- An employee, temporary worker, or contractor who complies in good faith with this policy is not subject to discipline under this policy.
- This policy does not prohibit an employee from accessing information about himself or herself as long as the person has been granted access to the system and uses authorized processes, or makes a request to OHFA for a list of the PII that the department maintains about himself or herself.

VIII. MAINTENANCE OF THIS POLICY

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects OHFA PII and systems.

IX. ATTACHMENTS

Request to Inspect Personal Information Procedure
Email Encryption for Outlook
Email Encryption for State of Ohio Webmail
Explanation for Exemption from Manual Logging of some OHFA Computer Systems

TABLE OF REVIEW DATE AND EFFECTIVE CHANGES

Number	Effective Date	Superseded/Modified	Significant Changes
C6	01/31/21	N/A	New Policy

OFFICE OF MULTIFAMILY HOUSING - DEVCO

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel or contractors of the Ohio Housing Finance Agency (OHFA) when accessing Confidential Personal Information (CPI) contained in DevCo which is managed by the Office of Multifamily Housing and maintained by OHFA Information Technology.

II. OVERVIEW

OHFA is required to comply with Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of CPI of individuals who may be receiving assistance from or work with OHFA and which information is stored in a state-maintained personal information system. Ohio Administrative Code (OAC) 175-10-02 regulates access to CPI. This procedure applies those rules to DevCo.

For purposes of this procedure:

- "Personal Information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential Personal Information," (CPI) is the data identified in section 3. H of this procedure.

III. SYSTEM DESCRIPTION

A. Name

DevCo

B. Description

DevCo is the enterprise application used by Office of Multifamily Housing to track compliance and incentive awards for all the multifamily funding programs administered by OHFA. DevCo is an n-tier, Microsoft .NET application running on a Windows Server and connected to a SQL Server database.

C. Purpose

The Office of Multifamily Housing uses DevCo primarily to maintain project records, contact information for the partners, developers and owners associated with them, as well as generate IRS 8609 forms and letters. In addition, DevCo is used to track compliance activities for active projects, store compliance information on buildings, units, and tenants, and generate IRS 8823 forms. The Devco system maintains information on roughly 2,900 projects, 6,100 awards, and 110,000 rental units in the system. Each unit has household members who must submit PI that is considered confidential in order to qualify for inhabiting the affordable or subsidized unit. Information is entered into DevCo by the property manager or owner of each project.

D. Regulatory Requirements

The information is collected to satisfy the regulations under; Internal Revenue Code Section 42, HUD's Tenant Data Collection Initiative (2008, HERA), ORC Chapter 174, 2013 HOME Final Rule, 24 CFR Part 92, 24 CFR Part 93, 24 CFR Part 891, 24 CFR Part 570, Internal Revenue Code Section 142, American Recovery and Reinvestment Act of 2009.

E. Authorizing Access

Access to DevCo CPI is based on a "need to know" basis for OHFA employees to fulfill his/her job duties. The determination of access to CPI will be approved by the employee's supervisor or the employee's Office Director prior to providing access to the system containing CPI. Upon approval access, the supervisor makes a request for access to IT via the IT Help Desk. IT then sets the rights accordingly. Authorizations are revoked at the request of the supervisor or when an employee leaves the program office or agency. Access is granted through a registration process for compliance staff of properties with OHFA funding by OHFA. (See DevCo Compliance User Guide for more information).

F. Security

Access to information in DevCo requires an account and a strong password. Employees must have access approved by the business unit primary contact and access is implemented by the IT Office. Periodic penetration tests are performed on this system by an approved security vendor to ensure it is compliant with the most recent application security standards.

G. Positions that Access the System

Position title	**Permission level** (Full access, limited access, etc.)	**CPI accessible with this permission level**	**Who Grants DevCo Online Permission**
Property Developers	Limited access to their own information	None	OHFA Development/T&TA
Property Owner	Limited access to their own information	Limited access to their own tenant information	OHFA Compliance/ T&TA
Property Manager	Limited access to their own information	Limited access to their own tenant information	Property Owner
Property Syndicator/Investor	Limited access to their own information (typically view only	Limited access to their own information (typically view only	Property Owner
OHFA Compliance Auditor	Full access	Yes	OHFA IT
OHFA Compliance Manager	Full access	Yes	OHFA IT
OHFA T&TA	Full access	Yes	OHFA IT
OHFA Development Analyst	Full access	Yes	OHFA IT
OHFA Development Manager	Full access	Yes	OHFA IT
OHFA IT	Full access	Yes	OHFA IT
Director of Housing Policy	Full access	Yes	OHFA IT
Research Analyst	Limited access	Yes	OHFA IT
Data Quality Assurance Coordinator	Limited access	Yes	OHFA IT
Director of Internal Audit	Limited access	No	OHFA IT
Chief Auditor	Limited access	No	OHFA IT
OHFA Call Center Personnel	Limited access	Yes	OHFA IT

H. Description of CPI contained in this System

Examples of information maintained in DevCo that identifies any individual who benefits directly or indirectly from financial assistance the agency provides such as:

- First and last name;
- Date of birth;
- Street address;
- Truncated (last 4) social security numbers; and
- Federal Tax Identification Numbers.

The system is a CPI system as defined under ORC section 1347.15

I. Valid Reasons for Accessing CPI

In accordance with OAC 175-10-03, there are valid reasons, directly related to OHFA's exercise of its powers or duties, for which only OHFA employees may access CPI regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of OHFA to access CPI:

- Responding to a public records request;
- Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;
- Complying with any state or federal program requirements;
- Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- Auditing purposes;
- Investigation or law enforcement purposes;
- Litigation, complying with an order of the court, or subpoena;
- Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leaverequests/issues, time card approvals/issues);
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;
- Complying with a collective bargaining agreement provision;
- Complying with any federal program requirements of programs administered by the agency; or
- Administering any program with individual participants or beneficiaries.

IV. LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

A. Logging Requirements

Logging is automated in DevCo therefore manual logging is not required.

i. **Automated logging**. Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

- **Application** – Name of the application generating the log;
- **Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY);
- **Time** – The time the event occurred (HH:MM:SS);
- **Time Zone** – GMT time and offset (if Time not in EST/EDT);
- **Username** – The name of the user accessing the application or attempting to access the application; and
- **Person** – The name/identifier of the person whose CPI was accessed.

V. REPORTING SUSPICIOUS OR INAPPROPRIATE REQUESTS

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See Incident Response for Access of Confidential Information for an Invalid Reason Procedure.

VI. TRAINING

A review of this procedure will be included on the agenda of scheduled policy updates and review meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing Devco which contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding OHFA policy.

VIII. ATTACHMENTS

Policy on Protecting Privacy (C6)
Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

IX. TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/21	New standard operating procedure

OHFA INFORMATION TECHNOLOGY OFFICE - DOCUWARE

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel or contractors of the Ohio Housing Finance Agency (OHFA) when accessing Confidential Personal Information (CPI) contained in DocuWare which is managed by the OHFA Information Technology Office.

II. OVERVIEW

OHFA is required to comply with Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of CPI of individuals who may be receiving assistance from or work with OHFA and which information is stored in a state-maintained personal information system. Ohio Administrative Code (OAC) 175-10-02 regulates access to CPI. This procedure applies those rules to DocuWare.

For purposes of this procedure:

- "Personal Information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential Personal Information," (CPI) is the data identified in section 3. H of this procedure.

III. SYSTEM DESCRIPTION

A. Name

DocuWare

B. Description

OHFA uses DocuWare software as its document management imaging system. DocuWare is a third party application running on Windows Server and utilizing SQL Server database.

C. Purpose

The system is used to house digital documentation consisting of home mortgage loan applications and supportive documentation, property and tenant information, vendor and purchasing information, as well as other miscellaneous information. The system represents original and official records of client applications, business contracts, and purchasing requisitions.

D. Regulatory Requirements

Internal Revenue Code Section 42, HUD's Tenant Data Collection Initiative (2008 HERA), 2013 HOME Final Rule, and 24 CFR Part 92, ORC 121.211, US Department of Treasury (SDO) and Section 143 of the Internal Revenue Code.

E. Authorizing Access

The IT Office grants access to DocuWare and assigns permissions on request by the employee's supervisor. Access to DocuWare is typically requested and tracked by the IT Help Desk whether it be for temporary access or access needed for the employee's job duties. When an employee terminates employment, access is revoked by disabling the employees OHFA network account. Access to DocuWare is granted by the Program manager.

F. *Security*

Access to information in DocuWare requires an account and a strong password. Employees must have access approved by the business unit primary contact and access is implemented by the IT Office. Periodic penetration tests are performed on this system by an approved security vendor to ensure it is compliant with the most recent application security standards.

G. *Positions that Access the System*

Position title	**Permission level** (Full access, limited access, etc.)	**CPI accessible with this permission level**
811 Program Coordinator	Limited Access	Yes
Administrative Professional I (8)	Limited Access	Yes
Administrative Professional II	Limited Access	Yes
Administrator Training & Technical Assistance	Limited Access	Yes
Architect	Limited Access	Yes
Asset Manager (2)	Limited Access	Yes
Asset Manager Portfolio Analyst	Limited Access	Yes
Assistant Director of Finance	Limited Access	Yes
Bond Accountant	Limited Access	Yes
Bond Accountant Coordinator	Limited Access	Yes
Bond Accountant II (7)	Limited Access	Yes
Budget and Contract Specialist	Limited Access	Yes
Budget Officer	Limited Access	Yes
Business Process Analyst I	Limited Access	Yes
Chief Auditor	Limited Access	No
Chief Executive Administrator	Limited Access	Yes
Chief Financial Officer	Limited Access	Yes
Chief Legal Counsel	Limited Access	Yes
CIO	Limited Access	Yes
Compliance Team Manager (2)	Limited Access	Yes
Controller	Limited Access	Yes
Data Quality Assurance Coordinator	Limited Access	Yes
Developer account with access to a test cabinet with a small amount of data that could contain CPI	Limited Access	Possibly
Director of Capital Markets	Limited Access	Yes
Director of Facilities	Limited Access	No
Director of Housing Policy	Limited Access	No
Director of Internal Audit	Limited Access	No
Director of Multifamily Housing	Limited Access	Yes
Executive Assistant	Limited Access	Yes
Fiscal Operations Manager	Limited Access	Yes

Position title	Permission level (Full access, limited access, etc.)	CPI accessible with this permission level
HHF Data Analyst	Limited Access	Yes
Housing Administrator	Limited Access	Yes
Housing Analyst II	Limited Access	Yes
Housing Development Analyst (9)	Limited Access	Yes
Housing Examiner (13)	Limited Access	Yes
Housing Examiner Trainee (2)	Limited Access	Yes
Housing Grant Analyst II (8)	Limited Access	Yes
Housing Preservation Center Assistant Manager	Limited Access	Yes
Housing Preservation Development Manager	Limited Access	Yes
Information Technologist II	Limited Access	Yes
Infrastructure Specialist I	Limited Access	Yes
Infrastructure Specialist II	Full Access	Yes
Infrastructure Specialist IV	Full Access	Yes
Legal Office Aide	Limited Access	Yes
Operations Manager	Limited Access	Yes
Planner II	Limited Access	Yes
Planner III (2)	Limited Access	Yes
Policy Administrator	Limited Access	Yes
Program & Policy Manager	Limited Access	Yes
Project Administration Manager	Limited Access	Yes
Project Portfolio Manager	Limited Access	Yes
Purchasing Supervisor	Limited Access	Yes
Rental Assistance Grant Specialist	Limited Access	Yes
Research Analyst	Limited Access	Yes
Single Family Homebuyer Manager	Limited Access	Yes
Senior Capital Markets Analyst	Limited Access	Yes
Single Family Accountant	Limited Access	Yes
Single Family Accounting Manager	Limited Access	Yes
Software Development Specialist III	Limited Access	Yes
Special Projects Coordinator	Limited Access	Yes
Sr. Housing Advisor for Housing Policies and Programs	Limited Access	Yes

H. Description of CPI contained in this System

Financial statements and data any person submits for any purpose to the Ohio Housing Finance Agency in connection with applying for, receiving, or accounting for financial assistance from the agency, and information that identifies any individual who benefits directly or indirectly from financial assistance from the agency; such as:

- First and last names;
- Date of birth;
- E-mail addresses;
- Street addresses;
- Social Security Numbers - including truncated SSNs;
- Federal Tax Identification Numbers;
- Financial information, ranging from account numbers, credit card numbers and debit card Numbers to credit history and credit scores; and
- Employment information.

The system is a CPI system as defined under ORC section 1347.15

I. Valid Reasons for Accessing CPI

In accordance with OAC 175-10-03, there are valid reasons, directly related to OHFA's exercise of its powers or duties, for which only OHFA employees may access CPI regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of OHFA to access CPI:

- Responding to a public records request;
- Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;
- Complying with any state or federal program requirements;
- Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- Auditing purposes;
- Investigation or law enforcement purposes;
- Litigation, complying with an order of the court, or subpoena;
- Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leaverequests/issues, time card approvals/issues);
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;
- Complying with a collective bargaining agreement provision;
- Complying with any federal program requirements of programs administered by the agency; or
- Administering any program with individual participants or beneficiaries.

IV. LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

A. Logging Requirements

Logging is automated in DocuWare therefore manual logging is not required.

i. **Automated logging**. Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

- **Application** – Name of the application generating the log;
- **Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY);
- **Time** – The time the event occurred (HH:MM:SS);
- **Time Zone** – GMT time and offset (if Time not in EST/EDT);
- **Username** – The name of the user accessing the application or attempting to access the application; and
- **Person** – The name/identifier of the person whose CPI was accessed.

V. REPORTING SUSPICIOUS OR INAPPROPRIATE REQUESTS

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure.

VI. TRAINING

A review of this procedure will be included on the OHFA agenda of regularly scheduled training meetings. In addition, new employees must receive training on this procedure prior to accessing DocuWare which contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding OHFA policies.

VIII. ATTACHMENTS

Policy on Protecting Privacy (C6)
Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

IX. TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/21	New standard operating procedure

FINANCE SYSTEMS

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel or contractors of the Ohio Housing Finance Agency (OHFA) when accessing Confidential Personal Information (CPI) contained in the Finance Systems which are managed by the Finance Office.

II. OVERVIEW

OHFA is required to comply with Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of CPI of individuals who may be receiving assistance from or work with OHFA and which information is stored in a state-maintained personal information system. Ohio Administrative Code (OAC) 175-10-02 regulates access to CPI. This procedure applies those rules to Finance Systems.

For purposes of this procedure:

- "Personal Information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential Personal Information," (CPI) is the data identified in section 3. H of this procedure.

III. SYSTEM DESCRIPTION

A. Name

Finance Systems

B. Description

The Finance Systems comprise three separate database applications with related functions: Emphasys, Innoprise, and GEMS. The systems are hosted on OHFA premises utilizing Microsoft servers and accessible via a private network. Users interact with the systems through Windows and intranet-only forms. Integration of data is accomplished manually by users through spreadsheets and automated database imports and exports.

C. Purpose

The Finance Systems are used by the agency for purchasing, making payments, employee reimbursements, general ledger reporting, and other transactions. Finance uses Emphasys to process bond transactions and associated second mortgages and some first mortgages for all bond issuances. The single family Homebuyer System Program's Emphasys module interfaces with the Finance Emphasys general ledger which in turn interfaces with the Finance's primary system, Innoprise. GEMS, an application used formerly as the general ledger system but now used only to process information on multifamily loan payments for import to Innoprise.

D. Regulatory Requirements

Chapter 175 of the Ohio Revised Code Section and 143 of the Internal Revenue Code.

E. Authorizing Access

Access to Finance Systems' CPI is based on a "need to know" basis for OHFA employees to fulfill his/her job duties. The determination of access to CPI will be approved by the employee's supervisor or the employee's CFO or his/her designee prior to providing access to the system containing CPI. Upon approval access, the supervisor makes a request for access to IT via the IT Help Desk. IT then sets the rights accordingly. Authorizations are revoked at the request of the supervisor or when an employee leaves the program office or agency.

F. *Security*

Access to the Finance Systems requires an account and strong password. Access Control Lists (ACLs) are used to limit availability of the sensitive data on a need-to-know basis only. Periodic penetration tests are performed on this system by an approved security vendor to ensure it is compliant with the most recent application security standards. The system supports access logging.

G. *Positions that Access the System*

Position title	**Permission level** (Full access, limited access, etc.)	**CPI accessible with this permission level**
Chief Financial Officer	Full	Yes
Assistant Director of Finance	Full	Yes
Controller	Full	Yes
Fiscal Operations Manager	Full	Yes
Single Family Accounting Manager	Limited	Yes
Budget Officer	Limited	Yes
Senior Accountant	Limited	Yes
Budget Coordinator	Limited	Yes
Purchasing Supervisor	Limited	Yes
Bond Accountant II	Limited	Yes
Bond Accountant Coordinator	Limited	Yes
Director of Internal Audit	Limited	No
Chief Auditor	Limited	No

H. *Description of CPI contained in this System*

Financial statements and data any person submits for any purpose to the Ohio Housing Finance Agency in connection with applying for, receiving, or accounting for financial assistance from the agency, and information that identifies any individual who benefits directly or indirectly from financial assistance from the agency; such as:

- First and last name;
- Date of birth;
- E-mail address;
- Street address;
- Social Security Numbers (including truncated SSNs);
- Federal Tax Identification Numbers;
- Financial information, ranging from account numbers, credit card numbers and debit card numbers to credit history and credit scores;
- Certificate/license numbers;
- Employment information; and
- Criminal information.

The system is a CPI system as defined under ORC section 1347.15

I. *Valid Reasons for Accessing CPI*

In accordance with OAC 175-10-03, there are valid reasons, directly related to OHFA's exercise of its powers or duties, for which only OHFA employees may access CPI regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of OHFA to access CPI:

- Responding to a public records request;
- Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;

- Complying with any state or federal program requirements;
- Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- Auditing purposes;
- Investigation or law enforcement purposes;
- Litigation, complying with an order of the court, or subpoena;
- Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leaverequests/issues, time card approvals/issues);
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;
- Complying with a collective bargaining agreement provision;
- Complying with any federal program requirements of programs administered by the agency; or
- Administering any program with individual participants or beneficiaries.

IV. LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

A. Manual Logging of Access to CPI

Manual logging of access to CPI applies whenever access is targeted to a specifically named individual or group of specifically named individuals. Manual logging does not apply when CPI is accessed for the following reasons:

i. **Self-service access or request to view own CPI**: No logging is necessary when a person views his or her own records containing CPI. For example, an agency customer who makes a request to review his or her case file would not trigger a logging requirement for a caseworker fulfilling the customer's request.

ii. **General Research**: When conducting general research, employees do not need to log access if the research is not directed toward a specific-named individual or a group of specifically named individuals. For example, running a report that lists licensees licensed from 2010 to 2019 and does not target a specifically named individual is excluded from the logging requirement.

iii. **Routine office procedures**: Logging is not required when performing routine office tasks that are not directed toward specific individuals or groups of specifically named individuals. For example, running a report that uses parameters other than names, such as dates, without the intention of retrieving the information of a specific employee is excluded from the logging requirement. However, using specific search parameters without a name but with the intent to retrieve a specifically named individual still triggers the logging requirement.

iv. **Incidental contact**: Logging is not required when an employee incidentally accesses CPI and the contact is merely a result of exposure to the information rather than the primary reason for the access. For example, if a desktop support employee is asked to correct a problem in a system and happens to see CPI because it is already on the screen, the desktop support employee is not required to log access to the CPI because the support employee is not targeting an individual's CPI.

v. **Information requested by an individual about that individual**: Logging is not required when an individual requests information about that individual. For example, if John Smith requests information on himself, no logging is required. The individual's request for action also serves as the individual's approval to access the information. In addition, "individual" means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual. Steps should be taken to ensure that the individual is authorized to make the request and has provided credentials for self or to affirm the relationship. (See also Explanation for Exemption from Manual Logging of some OHFA Computer Systems Memorandum).

vi. **Automated logging**: Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

- **Application** – Name of the application generating the log;
- **Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY);
- **Time** – The time the event occurred (HH:MM:SS);
- **Time Zone** – GMT time and offset (if Time not in EST/EDT);
- **Username** – The name of the user accessing the application or attempting to access the application; and
- **Person** – The name/identifier of the person whose CPI was accessed.

B. *Manual Logging*

The Finance Systems do not have automated logging, therefore OHFA employees must use the Log of Access to Confidential Personal Information form under the following conditions:

i. Access in a system containing CPI to accomplish job duties and the access is specifically directed toward a specifically named individual or a group of specifically named individuals.
ii. Access in a system containing CPI because of another state employee's request for information.
iii. Public record requests that require accessing a system containing CPI.
iv. Annual acknowledgement that CPI was not accessed for any invalid reasons.

C. *Use and Maintenance of a "Log of Access to Confidential Personal Information"*

Employees shall use the OHFA Log of Access to Confidential Personal Information form (CPI Log Form) available on the Intranet to list each incident when CPI has been accessed for those conditions listed above. Employees will log any invalid CPI access occurrence immediately, notify their manager of the occurrence, and maintain the CPI Log Form on his/her shared drive.

D. *Retention and destruction of a CPI Log Form*

New CPI Log Forms will be started at the beginning of each year for each system. At the end of each calendar year, or upon termination of employment, all OHFA employees and temporary personnel will sign off on their individual CPI Log Form and submit the form to his/her manager. The manager will submit the CPI Log Forms to the CIO for secure storage on the shared drive. The CPI Log Form files will be permanently deleted after three years.

V. REPORTING SUSPICIOUS OR INAPPROPRIATE REQUESTS

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure.

VI. TRAINING

A review of this procedure will be included on the agenda of OHFA meetings. In addition, new employees must receive training on this procedure prior to accessing the Finance Systems which contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15, and Ohio Administrative Code Section 175-10-01 through 175-10-05.

VIII. ATTACHMENTS

Explanation for Exemption from Manual Logging of some OHFA Computer Systems
Log of Access to Confidential Personal Information
Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure
Policy on Protecting Privacy (C6)

IX. TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/2021	New standard operating procedure

HARDEST HIT FUND (HHF) ALLITA 360

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel or contractors of the Ohio Housing Finance Agency (OHFA) when accessing Confidential Personal Information (CPI) contained in HHF Allita 360 which is managed by the Home Ownership Preservation Program.

II. OVERVIEW

OHFA is required to comply with Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of CPI of individuals who may be receiving assistance from or work with OHFA and which information is stored in a state-maintained personal information system. Ohio Administrative Code (OAC) 175-10-02 regulates access to CPI. This procedure applies those rules to HHF Allita 360.

For purposes of this procedure:

- "Personal Information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential Personal Information," (CPI) is the data identified in section 3. H of this procedure.

III. SYSTEM DESCRIPTION

A. Name

HHF Allita 360

B. Description

HHF Allita 360 is a secure web-based portal that interfaces with the OHFA DocuWare system which houses all documents pertaining to the homeowners' and land banks' files as well as fill-in fields that are used for collecting client/parcel specific attributes.

C. Purpose

The system is used for mandated data collection for grant programs, for use in providing funding to homeowners and land banks SDO-for processing of files to be funded for assistance; research, reporting to stakeholders, including the OHFA Board.

D. Regulatory Requirements

U.S. Department of Treasury TARP Program in accordance with the terms of the HHF program. Please note that the Department of Treasury created the HHF program for states hit particularly hard during the recent mortgage crisis and allocated $762.7 million to assist Ohio's distressed homeowners. By law, this program was to originally end in 2020, however, the program has been extended into 2021. Ohio expects to close out with the Treasury by September 30, 2021. Files and documents must be retained for three years after the last funding.

E. Authorizing Access

Access to HHF Allita 360 CPI is based on a "need to know" basis for OHFA employees to fulfill his/her job duties. The determination of access to CPI will be approved by the HHF Program Manager prior to providing access to the system containing CPI. The HHF Program Manager sets the rights accordingly. Authorizations are revoked by the HHF Program Manager or when an employee leaves the program office or agency.

F. Security

Access to the portal requires an account and strong password. Access Control Lists (ACLs) are used to limit availability of the sensitive data on a need-to-know basis only. Periodic penetration tests are performed on this system by an approved security vendor to ensure it is compliant with the most recent application security standards. The system supports access logging. Security to the HHF Allita 360 system is managed by the HHF Program Manager. Secured network, secured websites, privacy policy; privacy training occurs annually for SDO employees. Risks are mitigated by using the most recent application technology available; employing security technology (SSL encryption, password authentication); restricting access to CPI on a need-to-know basis only; and staff training on securing CPI. Data is obtainable only via the reporting tool that is built within the system or by accessing individual files, which are both protected by security layers; *Associate's Title* website is a data and communication warehouse used only for the retention of closing records; *"Contact Us" Fraud list* is a list created by data inputs from the consumer website. Homeowner information stored includes non-private data as well as information pertaining to the investigation.

G. Positions that Access the System

Position title	**Permission level** (Full access, limited access, etc.)	**CPI accessible with this permission level**
Housing Preservation Development Manager	Full	Yes
Housing Preservation Center Assistant Manager	Full	Yes
HHF Data Analyst	Full	Yes
Housing Development Analyst	Full	Yes
Administrative Professional I	Full	Yes
Research Analyst – Housing Policy	Full	Yes
Infrastructure Specialist IV	Full	Yes
Greenwood 360 - Contractor	Full	Yes
Switchbox – Contractor	Full	Yes
Save the Dream Participants	Limited to own information	Yes – own information
Single Family Homebuyer Manager	Limited Access	Yes
Senior Capital Markets Analyst	Limited Access	Yes
Single Family Accountant	Limited Access	Yes
Single Family Accounting Manager	Limited Access	Yes
Software Development Specialist III	Limited Access	Yes
Special Projects Coordinator	Limited Access	Yes
Sr. Housing Advisor for Housing Policies and Programs	Limited Access	Yes

H. *Description of CPI contained in this System*

Financial statements and data any person submits for any purpose to the Ohio Housing Finance Agency in connection with applying for, receiving, or accounting for financial assistance from the agency, and information that identifies any individual who benefits directly or indirectly from financial assistance from the agency; such as:

- First and last names;
- Dates of birth;
- Email addresses;
- Street addresses;
- Social Security Numbers;
- Federal Tax ID Numbers;
- Driver's license numbers or state identification card if no license;
- Bank account numbers;
- Health and medical information (if hardship);
- Employment information; and
- Criminal information (Dodd-Frank only).

The system is a CPI system as defined under ORC section 1347.15

I. *Valid Reasons for Accessing CPI*

In accordance with OAC 175-10-03, there are valid reasons, directly related to OHFA's exercise of its powers or duties, for which only OHFA employees may access CPI regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of OHFA to access CPI:

- Responding to a public records request;
- Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;
- Complying with any state or federal program requirements;
- Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- Auditing purposes;
- Investigation or law enforcement purposes;
- Litigation, complying with an order of the court, or subpoena;
- Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leaverequests/issues, time card approvals/issues);
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;
- Complying with a collective bargaining agreement provision;
- Complying with any federal program requirements of programs administered by the agency; or
- Administering any program with individual participants or beneficiaries.

IV. LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

A. Logging Requirements

Logging is automated in the HHF Allita 360 System, therefore manual logging is not required.

i. **Automated logging**. Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

- **Application** – Name of the application generating the log;
- **Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY);
- **Time** – The time the event occurred (HH:MM:SS);
- **Time Zone** – GMT time and offset (if Time not in EST/EDT);
- **Username** – The name of the user accessing the application or attempting to access the application; and
- **Person** – The name/identifier of the person whose CPI was accessed.

V. REPORTING SUSPICIOUS OR INAPPROPRIATE REQUESTS

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure.

VI. TRAINING

A review of this procedure will be included on the agenda of OHFA meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing the HHF Allita 360 system which contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding OHFA policies.

VIII. ATTACHMENTS

Policy on Protecting Privacy (C6)
Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

IX. TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/21	New standard operating procedure

MULTIFAMILY PROGRAM COMPLIANCE SYSTEM – ALLITA 360

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel or contractors of the Ohio Housing Finance Agency (OHFA) when accessing Confidential Personal Information (CPI) contained in Multifamily Program Compliance System – Allita 360 (Allita 360) which is managed by the Multifamily Program.

II. OVERVIEW

OHFA is required to comply with Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of CPI of individuals who may be receiving assistance from or work with OHFA and which information is stored in a state-maintained personal information system. Ohio Administrative Code (OAC) 175-10-02 regulates access to CPI. This procedure applies those rules to Allita 360.

For purposes of this procedure:

- "Personal Information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential Personal Information," (CPI) is the data identified in section 3. H of this procedure.

III. SYSTEM DESCRIPTION

A. Name

Multifamily Program Compliance System – Allita 360 (Allita 360)

B. Description

The Allita 360 program consists of two phases of which the compliance staff utilize in order to conduct compliance audits. The software allows OHFA to conduct on-site physical and file inspections of LIHTC and other state and federal funded projects utilizing an iPad to be most efficient. This same system is used to create reports and allow for the owner/manager to submit documentation to support the correction of compliance issues.

C. Purpose

Allita 360 enables compliance staff to audit owner compliance with housing regulations, rules and codes related to housing low-income households and maintaining their projects in a safe manor. The information in the system includes project, owner, management and tenant data and non-compliance findings. Typical transactions include creating record of non-compliance, creating audit reports and reviewing to owners who submit corrective actions.

D. Regulatory Requirements

OHFA ORC Chapter 175; Section 42 Tax Credit Program. Low Income Housing Tax Credit (LIHTC) program regulations are under Section 42 of the IRS Code.

E. Authorizing Access

Access to Allita 360 CPI is based on a "need to know" basis for OHFA employees to fulfill his/her job duties. The determination of access to CPI will be approved by the employee's supervisor or the employee's Office Director prior to providing access to the system containing CPI. Upon approval access, the supervisor makes a request for access to IT via the IT Help Desk. IT then sets the rights accordingly. Authorizations are revoked at the request of the supervisor or when an employee leaves the program office or agency.

F. *Security*

Allita 360 uses the most recent application technology available employing security technology (SSL encryption, password authentication); restricting access to CPI on a need-to-know basis only; HUD relaxed reporting requirements on tenant personal characteristics such as requiring only the last four digits of a tenant's SSN; and staff training on securing CPI.

G. *Positions that Access the System*

Position title	**Permission level** (Full access, limited access, etc.)	**CPI accessible with this permission level**
Compliance Operations Manager	Full access	Yes
Project Transition Manager	Full access	Yes
Compliance Coordinator	Full access	Yes
Compliance Review Coordinator	Full access	Yes
Administrative Professional I	Full access	Yes
Housing Examiner	Full access	Yes
Housing Examiner Trainee	Full access	Yes
Greenwood 360 – Contractor	Full access	Yes

H. *Description of CPI contained in this System*

Financial statements and data any person submits for any purpose to the Ohio Housing Finance Agency in connection with applying for, receiving, or accounting for financial assistance from the agency, and information that identifies any individual who benefits directly or indirectly from financial assistance from the agency; such as:

- First and last names;
- Dates of birth;
- Email addresses;
- Street addresses;
- Social Security Numbers;
- Federal Tax ID Numbers;
- Financial information, ranging from account numbers, credit card numbers and debit card numbers to credit history and credit scores;
- Student identification numbers;
- Health and medical information, ranging from medical account numbers and health plan numbers to diagnoses, health conditions and drug prescriptions;
- Certificate/license numbers;
- Employment information;
- Criminal information; and
- Vehicle identifier including license plate.

The system is a CPI system as defined under ORC section 1347.15

I. *Valid Reasons for Accessing CPI*

In accordance with OAC 175-10-03, there are valid reasons, directly related to OHFA's exercise of its powers or duties, for which only OHFA employees may access CPI regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of OHFA to access CPI:

- Responding to a public records request;
- Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;
- Complying with any state or federal program requirements;
- Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- Auditing purposes;
- Investigation or law enforcement purposes;
- Litigation, complying with an order of the court, or subpoena;
- Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leaverequests/ issues, time card approvals/issues);
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;
- Complying with a collective bargaining agreement provision;
- Complying with any federal program requirements of programs administered by the agency; or
- Administering any program with individual participants or beneficiaries.

IV. LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

A. Logging Requirements

Logging is automated in the Multifamily Program Compliance System Allita 360, therefore manual logging is not required.

i. **Automated logging**. Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

- **Application** – Name of the application generating the log;
- **Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY);
- **Time** – The time the event occurred (HH:MM:SS);
- **Time Zone** – GMT time and offset (if Time not in EST/EDT);
- **Username** – The name of the user accessing the application or attempting to access the application; and
- **Person** – The name/identifier of the person whose CPI was accessed.

V. REPORTING SUSPICIOUS OR INAPPROPRIATE REQUESTS

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See Incident Response for Access of Confidential Information for an Invalid Reason Procedure.

VI. TRAINING

A review of this procedure will be included on the agenda of scheduled policy updates and review meetings. In addition, new employees must receive training on this standard operating procedure prior to accessing Allita 360 which contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15 and with any corresponding OHFA policy.

VIII. ATTACHMENTS

Policy on Protecting Privacy (C6)
Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

IX. TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/21	New standard operating procedure

RESIDENTIAL LENDING DIVISION – HOMEBUYER PROGRAM SYSTEM

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel or contractors of the Ohio Housing Finance Agency (OHFA) when accessing Confidential Personal Information (CPI) contained in the Residential Lending Division – Homebuyer Program System which is managed by the Office of Single Family Housing – Residential Lending Division.

II. OVERVIEW

OHFA is required to comply with Ohio Revised Code Section 1347.15 which includes provisions to protect the privacy and security of CPI of individuals who may be receiving assistance from or work with OHFA and which information is stored in a state-maintained personal information system. Ohio Administrative Code (OAC) 175-10-02 regulates access to CPI. This procedure applies those rules to the Residential Lending Division – Homebuyer Program System.

For purposes of this procedure:

- "Personal Information," as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- "Confidential Personal Information," (CPI) is the data identified in section 3. H of this procedure.

III. SYSTEM DESCRIPTION

A. Name

Residential Lending Division – Homebuyer Program System

B. Description

OHFA operates the First-Time Homebuyer, Lender Online Reservation System (LORS) and several subcompact systems that support it to make up the Residential Lending Division – Homebuyer Program System. This system is owned by the OHFA through a license agreement with AOD/Emphasys, the primary solution provider of systems that support many state housing finance agencies first-time homebuyer products.

General Description of Modules: The Lender Online Reservation System (LORS) and its subcomponent systems support OHFA's flagship program, the First-Time Homebuyer program. LORS is a secure web portal whereby financial institutions and OHFA's division of Homeownership process homebuyer mortgage loans. Primary functions include entering reservations, checking loan statuses, running reports, and checking allocation statuses, all via the internet.

Secondary subcomponent and supportive systems include the Homebuyer Education Portal (HBE) and Loan Tracking/Single Family Systems. Homebuyers are directed to the HBE portal where they must complete streamline homebuyer education, if they did not attend classes with a local HUD approved counseling agency. Loan Tracking (LT)/Single Family (SF) systems are utilized by Homeownership staff to monitor and ensure compliance to program guidelines.

C. Purpose

The primary purpose of LORS is to provide the technology necessary to support the agency's mission of expanding access to homeownership opportunities for first-time homebuyers and low to moderate income households throughout Ohio. To date, OHFA has helped over 145,000 first-time homebuyers, most of which are maintained and retained on the Lender Online Reservation System or one of its subsystems.

D. Regulatory Requirements

Authority to operate this program is cited in the Agency's duties and powers in the Ohio Revised Code Chapter 175 Housing Finance Agency. When bond proceeds are used, the agency is following Section 143 of the Internal Revenue Code to ensure compliance. We have elected to apply the same criteria to market rate loan programs as well to stay consistent and to comply with agency and program guidelines.

E. Authorizing Access

Access to the Residential Lending Division – Homebuyer Program System CPI is based on a "need to know" basis for OHFA employees to fulfill his/her job duties. The determination of access to CPI will be approved by the employee's supervisor or the employee's Office Director prior to providing access to the system containing CPI. Upon approval access, the supervisor makes a request for access to IT via the IT Help Desk. IT then sets the rights accordingly. Authorizations are revoked at the request of the supervisor or when an employee leaves the program office or agency.

F. Security

Procedures are documented in the system. Each manager sets the access level for their staff. The system tracks all changes made by staff and logs all access to individual records and data fields. Managers have access to print these reports.

The risk is mitigated by providing a secure web portal that is SSL (Secure Socket Layer) protected, which means data on the portal site is encrypted and not readable as it is exchanged by authorized users of the system. Access to the portal requires an account and strong password. Access Control Lists (ACLs) are used to limit availability of the sensitive data on a need-to-know basis only. Periodic penetration test are performed on this system by an approved security vender, the most recent in June 2018, to ensure it is compliant with the most recent application security standards.

Accounts, passwords, access control lists are used to limit exposure and access to data. The system also accommodates granular access to sensitive data. Built-in validation checks to ensure accuracy. Requests for data or reports must be entered into the Agency's help desk system, which requires several supervisory approval levels.

Risks are mitigated by using the most recent application technology available; employing security technology (SSL encryption, password authentication); restricting access to CPI on a need-to-know basis only; and staff training on securing CPI.

G. Positions that Access the System

Position title	**Permission level** (Full access, limited access, etc.)	**CPI accessible with this permission level**
Single Family Homebuyer Manager	Full access	Yes
Housing Preservation Manager	Full access	Yes
Administrative Professional I	Full access	Yes
Administrative Professional II	Limited	Yes
Bond Accountant Coordinator	Full access	Yes
Housing Development Analyst	Limited	Yes
Director of Housing Policy	Limited Access	No
Controller	Limited Access	Yes
Single Family Accounting Manager	Limited Access	Yes

H. Description of CPI Contained in this System

Financial statements and data any person submits for any purpose to the Ohio Housing Finance Agency in connection with applying for, receiving, or accounting for financial assistance from the agency, and information that identifies any individual who benefits directly or indirectly from financial assistance from the agency; such as:

- First mortgage characteristics;
- Borrower and Coborrower – age;
- Social Security Numbers;
- Federal Tax ID Numbers;
- Date of birth;
- Ethnicity;
- Credit history;
- Credit scores;
- Financial information;
- Certificate/license numbers;
- Criminal information;
- Income;
- Household data;
- Street address; and
- Property to be purchased information.

The system is a CPI system as defined under ORC section 1347.15.

I. Valid Reasons for Accessing CPI

In accordance with OAC 175-10-03, there are valid reasons, directly related to OHFA's exercise of its powers or duties, for which only OHFA employees may access CPI regardless of whether the personal information system is a manual system or computer system. Performing the following functions constitute valid reasons for authorized employees of OHFA to access CPI:

- Responding to a public records request;
- Responding to a request from an individual for the list of CPI the agency maintains on that individual;
- Administering a constitutional provision or duty;
- Administering a statutory provision or duty;
- Administering an administrative rule provision or duty;
- Complying with any state or federal program requirements;
- Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- Auditing purposes;
- Investigation or law enforcement purposes;
- Litigation, complying with an order of the court, or subpoena;
- Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/ issues, time card approvals/issues);
- Complying with an executive order or policy;
- Complying with an agency policy or a state administrative policy issued by the department of administrative services, the officeof budget and management or other similar state agency;
- Complying with a collective bargaining agreement provision;
- Complying with any federal program requirements of programs administered by the agency; or
- Administering any program with individual participants or beneficiaries.

IV. LOGGING ACCESS TO CONFIDENTIAL PERSONAL INFORMATION

A. Manual Logging of Access to CPI

Manual logging of access to CPI applies whenever access is targeted to a specifically named individual or group of specifically named individuals. Manual logging does not apply when CPI is accessed for the following reasons:

i. **Self-service access or request to view own CPI**. No logging is necessary when a person views his or her own records containing CPI. For example, an agency customer who makes a request to review his or her case file would not trigger a logging requirement for a caseworker fulfilling the customer's request.

ii. **General Research**. When conducting general research, employees do not need to log access if the research is not directed toward a specific-named individual or a group of specifically named individuals. For example, running a report that lists licensees licensed from 2010 to 2019 and does not target a specifically named individual is excluded from the logging requirement.

iii. **Routine office procedures**. Logging is not required when performing routine office tasks that are not directed toward specific individuals or groups of specifically named individuals. For example, running a report that uses parameters other than names, such as dates, without the intention of retrieving the information of a specific employee is excluded from the logging requirement. However, using specific search parameters without a name but with the intent to retrieve a specifically named individual still triggers the logging requirement.

iv. **Incidental contact**. Logging is not required when an employee incidentally accesses CPI and the contact is merely a result of exposure to the information rather than the primary reason for the access. For example, if a desktop support employee is asked to correct a problem in a system and happens to see CPI because it is already on the screen, the desktop support employee is not required to log access to the CPI because the support employee is not targeting an individual's CPI.

v. **Information requested by an individual about that individual**. Logging is not required when an individual requests information about that individual. For example, if John Smith requests information on himself, no logging is required. The individual's request for action also serves as the individual's approval to access the information. In addition, "individual" means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual. Steps should be taken to ensure that the individual is authorized to make the request and has provided credentials for self or to affirm the relationship. (See also Explanation for Exemption from Manual Logging of some OHFA Computer Systems Memorandum).

vi. **Automated logging**: Manual logging is not required when the user's access to CPI is recorded by an automated mechanism. Any upgrade of a system or acquisition of a new system must include an automated recording mechanism. This mechanism shall include:

- **Application** – Name of the application generating the log;
- **Date** – The date an event occurred (format should be standardized, such as DD-MM-YYYY or MM-DD-YYYY);
- **Time** – The time the event occurred (HH:MM:SS);
- **Time Zone** – GMT time and offset (if Time not in EST/EDT);
- **Username** – The name of the user accessing the application or attempting to access the application; and
- **Person** – The name/identifier of the person whose CPI was accessed.

B. Manual Logging

The Residential Lending Division – Homebuyer Program System does not have automated logging, therefore OHFA employees must use the **Log of Access to Confidential Personal Information form** under the following conditions:

i. Access in a system containing CPI to accomplish job duties and the access is specifically directed toward a specifically named individual or a group of specifically named individuals.

ii. Access in a system containing CPI because of another state employee's request for information.

iii. Public record requests that require accessing a system containing CPI.

iv. Annual acknowledgement that CPI was not accessed for any invalid reasons.

C. Use and Maintenance of a "Log of Access to Confidential Personal Information"

Employees shall use the OHFA Log of Access to Confidential Personal Information form (CPI Log Form) available on the Intranet to list each incident when CPI has been accessed for those conditions listed above. Employees will log any invalid CPI access occurrence immediately, notify his/her manager of the occurrence, and will maintain the CPI Log Form on his/her shared drive.

D. Retention and destruction of a CPI Log Form

New CPI Log Forms will be started at the beginning of each calendar year for each system. At the end of each calendar year, or upon termination of employment, all OHFA employees will sign off on their individual CPI Log Form and submit the forms to his/her manager. The manager will submit the CPI Log Forms to the CIO for secure storage on the shared drive. The CPI Log Form files will be permanently deleted after three years.

V. REPORTING SUSPICIOUS OR INAPPROPRIATE REQUESTS

Employees are required to immediately report any suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of this procedure or the Policy on Protecting Privacy. See Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure.

VI. TRAINING

A review of this procedure will be included on the OHFA agenda of regularly scheduled training meetings. In addition, new employees must receive training on this procedure prior to accessing the Residential Lending Division – Homebuyer Program System which contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Section 1347.15, and Ohio Administrative Code Section 175-10-01 through 175-10-05.

VIII. ATTACHMENTS

Explanation for Exemption from Manual Logging of some OHFA Computer Systems
Log of Access to Confidential Personal Information
Policy on Protecting Privacy (C6)
Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

IX. TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/21	New standard operating procedure

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by employees, temporary personnel and contractors of the Ohio Housing Finance Agency (OHFA) when responding to written requests to inspect Personal Information (PI) contained in a system managed by OHFA.

II. OVERVIEW

In accordance with Ohio Revised Code (ORC) 1347.08(A), upon the request of a properly identified person, every state agency that maintains a personal information system must:

- inform that person of the existence of any personal information about him or her in the system;
- permit the person to inspect that personal information in the system(s); and
- inform the person about the types of uses made of the personal information and the identity of users granted access.

Exceptions to ORC 1347.08 also exist and must be considered.

ORC Section 1347.15(B)(5) requires state agencies to comply with a written request from an individual for a list of Confidential Personal Information (CPI) about the individual that the state agency keeps, unless the CPI relates to an investigation about the individual based upon specific statutory authority.

III. DEFINITIONS

Individual - means a natural person, an authorized representative, legal counsel, legal custodian or legal guardian of the individual.

Personal information - as defined by Ohio Revised Code (ORC) 1347.01, means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person. Some examples of "personal information" can include but are not limited to the following:

- names
- Social Security numbers
- resumes
- contracts
- correspondence
- addresses
- phone numbers
- driver's license numbers
- state identification numbers
- professional license numbers
- financial account information
- medical and health information
- physical characteristics and other biometric information
- education information
- tax information
- individuals' job classifications and salary information
- performance evaluations
- employment application forms
- timesheet

Confidential Personal Information (CPI) - Personal information that falls within the scope of section 1347.15 of the Revised Code and that OHFA is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, medical and health information, financial statements and data submitted for any purpose to OHFA by any person in connection with applying for, receiving, or accounting for financial assistance the agency provides; and information that identifies any individual who benefits directly or indirectly from financial assistance the agency provides that could be maintained in one of the following seven personal information systems:

- DevCo;
- DocuWare;
- Finance Systems;
- Hardest Hit Fund - Allita 360;
- Multifamily Program Compliance - Allita 360;
- Residential Lending Division – Homebuyer Program; and
- Human Resources – Employee and Applicant Records.

IV. REQUESTS TO INSPECT PERSONAL INFORMATION

A. *Evaluate the Request*

As a standard practice, general requests from individuals to review their own personal information should be routed to the OHFA Chief Legal Counsel for evaluation. The requester must put the request for personal information in writing. Individual OHFA offices may have specific business processes that involve the collection, verification or communication with customers regarding their personal information. This procedure does not supersede those business processes as long as those business processes are consistent with ORC Chapter 1347 in providing individuals with an opportunity to review their personal information.

B. *Verify the Identity of the Requester*

If the personal information entirely constitutes a public record subject to disclosure under ORC 149.43, then it will be disclosed in accordance with the Public Records Request Policy D5. For personal information that is not a public record, however, the subject of the information still has a right, with some limitations, to review his or her own information under ORC Chapter 1347.

If the personal information constitutes CPI, then the law prohibits the agency from releasing the information except to certain parties. For this reason, the Chief Legal Counsel must verify the identity of the requester of the CPI to ensure that fulfilling the request is appropriate. To verify the requester's identity, the requester must appear in person and present a valid driver's license, official state identification card or passport. In the event an individual cannot present one of those three photo IDs, the department may accept a similarly trustworthy form of verification. Use of an alternative form of verification shall be approved by the Chief Legal Counsel prior to release of the CPI.

C. *Limitations on Disclosure*

The Chief Legal Counsel must determine if there are any requirements pertaining to the disclosure of the PI or CPI or any legal restriction that limits the release of the PI or CPI to the subject of the information. Some examples include:

- OHFA is not required to release any CPI under ORC 1347.15 that relates to an investigation about that individual.
- The Chief Legal Counsel, must disclose medical, psychiatric, or psychological information to a person who is the subject of the information or to the person's legal guardian, unless a physician, psychiatrist, or psychologist determines for the agency that the disclosure of the information is likely to have an adverse effect on the person. In this case, the information shall be released to a physician, psychiatrist, or psychologist who is designated by the person or by the person's legal guardian.
- OHFA must not release a confidential law enforcement investigatory record or trial preparation record as defined in divisions (A)(2) and (4) of section 149.43 of the Revised Code.
- OHFA is not required to release any personal information about an individual if the information is excluded from the scope of Chapter 1347 of the Revised Code.

D. *Dispose the Request*

Personal information is to be available for inspection during regular business hours, with the exception of published holidays. Personal information must be made available for inspection promptly. Copies of personal information must be made available within a reasonable period of time. "Prompt" and "reasonable" take into account the volume of personal information requested; the proximity of the location where the information is stored; and the necessity for any legal review of the information requested.

Each request should be evaluated for an estimated length of time required to gather the personal information. All requests for personal information must be satisfied within a reasonable time.

V. COSTS FOR PERSONAL INFORMATION

Those seeking personal information may be charged only the actual cost of making copies. The standard charge for paper copies is 5 cents per page.

Requesters may ask that records be mailed to them. They will be charged the actual cost of postage and mailing supplies. The office may require the requester to pay the cost of providing the information in advance. Electronic sensitive personally identifiable information must be sent to the requester in an encrypted format. The means of decrypting the information shall be sent through a separate communication.

VI. QUESTIONS

For questions regarding this policy, please contact the Chief Legal Counsel.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC Sections 1347.08 and 1347.15 and with any corresponding OHFA policy.

VIII.TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/2021	New procedure

OHIO HOUSING FINANCE AGENCY

What is Zix email encryption and when should you use it?

Email use poses a risk of unintended disclosure of information. Many emails are currently transmitted in clear (not encrypted) form. By means of some available tools, persons other than the designated recipients can read the email contents and attachments.

Email encryption is encryption of email messages (and attachments) to protect the content from being read by other entities than the intended recipients.

The State of Ohio has chosen a product called **Zix Email Encryption** for employees to use to encrypt emails with sensitive information. This software provides end to end encryption to protect emails and attachments.

When it should be used:

Email encryption should be used whenever sensitive information is sent over email. Sensitive information is defined as data that can be traced back to an individual and that, if disclosed, could result in harm to that person.

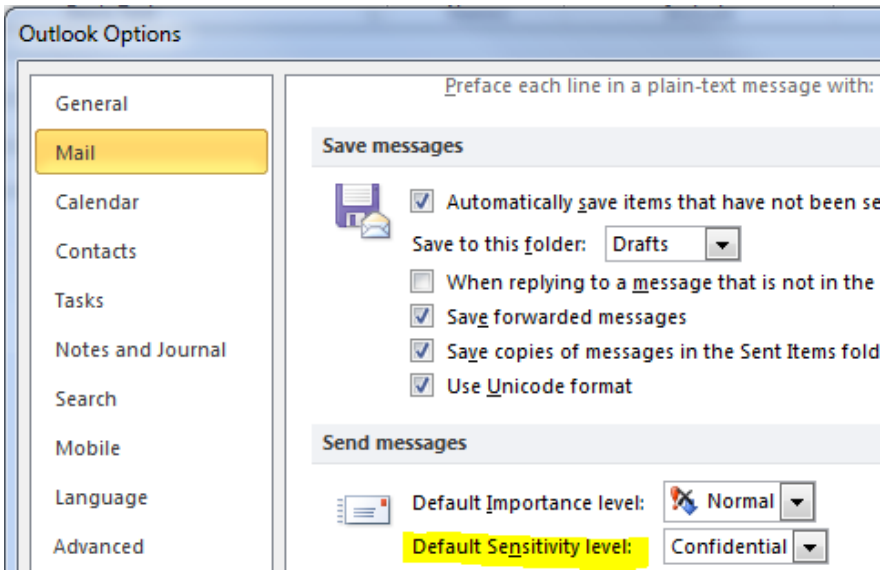
How to use it:

Zix Email Encryption should be installed on all OHFA workstations. There are 2 ways of using Zix.

1. When composing a message you will see an addition send button in the button bar above the standard send button. This button will have a padlock image with "Encrypt & Send" below it. Once you have drafted an email with sensitive information you would use this button to send the email and the Zix software will automatically detect which encryption method to use to ensure it is encrypted when sending the email.

(Bear in mind that the Zix button sends the email immediately, taking the place of the normal, unencrypting "Send" button.)

2. Setting the sensitivity of the message to **Confidential**. Select the File menu option on a new message window, then click "Options." Under the "Send Messages" section, change the "Default Sensitivity level" to "Confidential."



This forces Outlook to send the email using the second transfer method mentioned below.

How it works & what to expect:

Zix encrypts and transfers emails in 2 ways.

Method 1: The first is using Transport Layer Security (TLS). This protocol works much like secure web browsing in that it creates a secure connection between 2 points before any information is transferred. This method is transparent to the sender and recipient as the email is securely delivered to the recipients mailbox with no additional actions needed.

Method 2: The second method is an inbox hosted by Zix on their email server. This method will send an email to the recipient with a link to the Zix Message Center where they will need to set up an account. Once the account is set up the recipient can then retrieve the message and attachments. They can also use this portal to send responses back to you ensuring the conversation is secure. This communication method does have a time limit of 15 days from the original message.

Sending Encrypted Emails Through State of Ohio Webmail

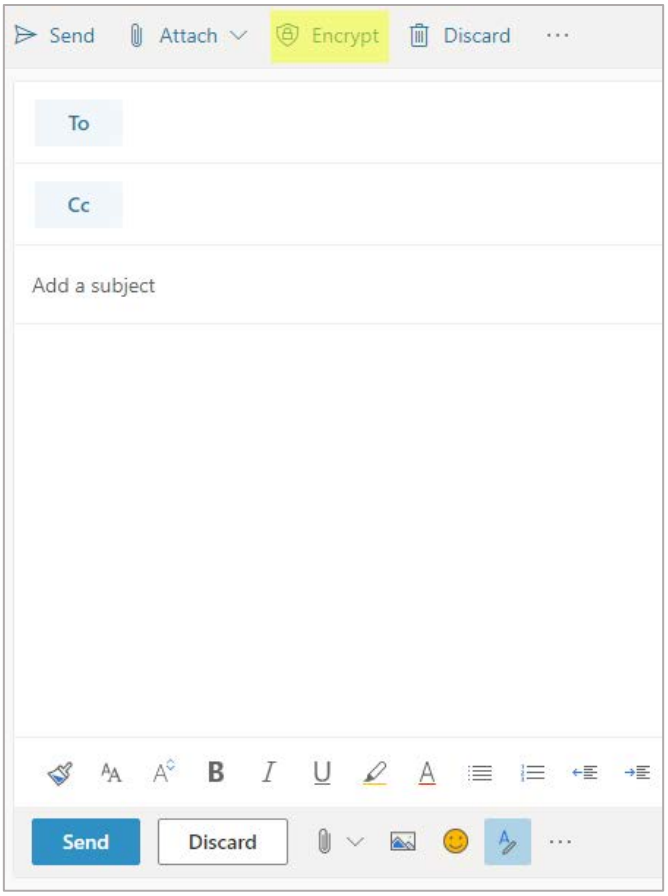
Whenever possible, you should avoid sending sensitive data or PII (personally identifiable information) through emails – whether in the body of the email or as attachments. When it isn't possible, you must use encryption.

Webmail Encryption

There are two methods to send encrypted emails through Webmail (https://webmail.ohio.gov):

Method 1. Use the "Encrypt" button

A. At the top of the new email you're drafting, there is a button named "Encrypt"



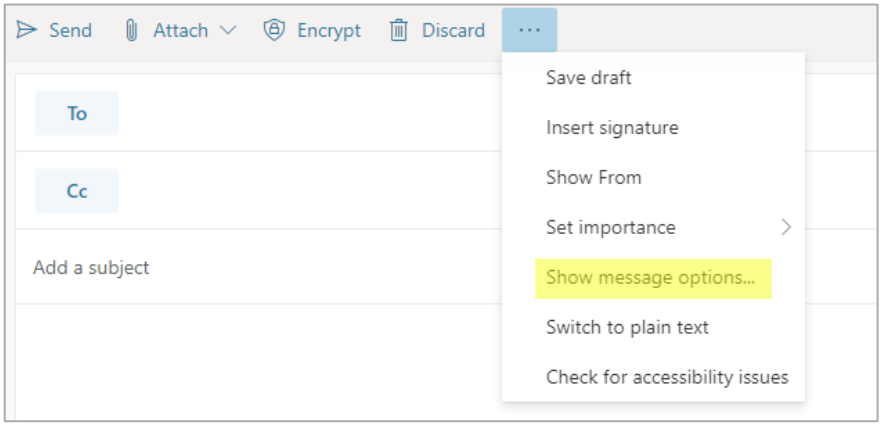
B. Click "Encrypt", write your email, attach files as necessary, then click "Send"

(continued on next page)

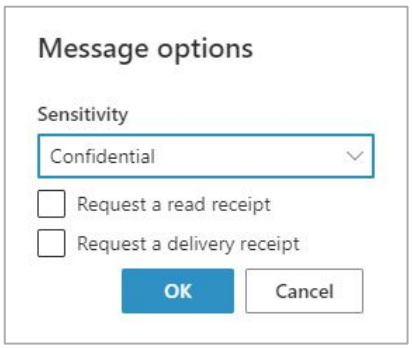
Method 2. Send as “Confidential” Email

A. From the draft email window, click the 3 dots “…”

B. Select “Show message options…” from the context menu



C. Set the “Sensitivity” to “Confidential”, then click “OK.”



D. Write your email, attach files as necessary, then click “Send”

If you have questions on any of the above, please call the IT Help Desk at 614-466-0489 or submit a Help Desk ticket.

I. PURPOSE

This standard operating procedure includes guidance and instructions that must be followed by the employees, temporary personnel, or contractors of the Ohio Housing Finance Agency (OHFA) when Confidential Personal Information (CPI) that is contained in an OHFA-managed system is accessed for an invalid reason by an OHFA employee, temporary worker or contractor. This document sets forth the procedures for processing illegal activity and wrongdoing, and provides for the careful, expeditious handling of all allegations and claims of improper access. The procedure covers both electronic and paper-based CPI.

II. OVERVIEW

Ohio Revised Code Section (ORC) 1347.15 (B) (6) requires a state agency to have a procedure to notify each person whose CPI has been accessed for an invalid reason by employees of the state agency. Depending on the circumstances, state and Federal laws require notification of affected individuals when there has been a security breach or invalid access for particular types of PII. However, it is not always clear whether a given incident is in fact a breach or other notification-triggering event.

III. DEFINITIONS

For purposes of this procedure:

Personally Identifiable Information (PII) - Information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

It includes "personal information" as defined by ORC 1347.01. Some examples of personally identifiable information can be but is not limited to the following:

- names
- Social Security numbers
- resumes
- contracts
- correspondence
- addresses
- phone numbers
- driver's license numbers
- state identification numbers
- professional license numbers
- financial account information
- medical and health information
- physical characteristics and other biometric information
- education information
- tax information
- individuals' job classifications and salary information
- performance evaluations
- employment application forms
- timesheets

Confidential Personal Information (CPI) - Personal information that falls within the scope of section 1347.15 of the Revised Code and that OHFA is prohibited from releasing under Ohio's public records law. It applies to Social Security numbers, medical and health information, financial statements and data submitted for any purpose to OHFA by any person in connection with applying for, receiving, or accounting for financial assistance the agency provides; and information that identifies any individual who benefits directly or indirectly from financial assistance the agency provides that is maintained in the no less than one of the following seven personal information systems:

- DevCo
- DocuWare
- Finance Systems
- Hardest Hit Fund - Allita 360
- Multifamily Program Compliance - Allita 360
- Residential Lending Division – Homebuyer Program System
- Human Resources – Employee and Applicant Records – paper-based

Illegal Activity - Includes fraud, theft, assault and other violations of local, state or federal law, including violations of state ethics laws, committed or in the process of being committed, by a state employee on any property owned or leased by the state or during the course of executing official duties.

Incident - Facts and circumstances that lead to a reasonable belief that there has been an access of CPI for an invalid reason that affects one or more computer systems, networks, or other components of the OHFA technology infrastructure, or to the threat of such an event.

Invalid Reason - Any basis for access to CPI that is not directly related to OHFA's exercise of its powers or duties as described in the agency's CPI access policies. Ohio Administrative Code 175-10-03 identifies valid reasons for accessing CPI within OHFA.

Wrongdoing - Includes a serious act or omission, committed by a state employee on any property owned or leased by the state or during the course of executing official duties. Wrongdoing is conduct that is not in accordance with standards of proper governmental conduct and which tends to subvert the process of government, including, but not limited, to gross violations of departmental or agency policies and procedures, executive orders, and acts of mismanagement, serious abuses of time, and other serious misconduct. For purposes of this reporting procedure, wrongdoing does not include illegal or suspected illegal activity. Likewise, wrongdoing does not include activity that is most appropriately handled through the department's human resources personnel.

IV. RESPONSE TO ACCESS OF CPI FOR AN INVALID REASON

A. Responsibilities

OHFA employees, temporary personnel and contractors have the following responsibilities when making a report of suspicious or inappropriate actions where it is perceived that CPI may have been requested or accessed for non-business reasons in violations of Accessing and Logging Confidential Personal Information procedures or the Policy on Protecting Privacy:

a. Report incidents of suspected access of CPI for an invalid reason to a manager. If unable to report the suspected incident to a manager, the report should be made to the OHFA CIO acting as the Data Privacy Point of Contact (DPPOC), Chief Legal Counsel or the system contact person for the program area involved.

b. Managers or the party that received the initial report shall notify the DPPOC of the suspected incident at 614-644-2444.

c. The DPPOC shall notify the Executive Director that a suspected incident has occurred and will be reviewed. The DPPOC will then coordinate a review of the suspected incident to determine if:

   iv. A security breach as defined by ORC 1347.12 has occurred, where "breach" is defined as unauthorized access to computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

   v. A violation of ORC 1347.15 has occurred, where CPI has been accessed for an invalid reason by an agency employee.

   vi. A violation of another regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), has occurred, or that there is some other risk or threat that makes notification of affected parties appropriate.

   The DPPOC will involve the following parties in this review:

   - Agency human resources representative;
   - System contact person for the program area involved;
   - Agency Chief Legal Counsel; and
   - Other parties as deemed appropriate.

g. If the review of the suspected incident determines that CPI has been inappropriately accessed, the Chief Legal Counsel shall report the incident in the following manner:

   - Notify the OHFA Executive Director.
   - Notify the Governor's Office.
   - Notify the Ohio Customer Service and Security Center (OCSSC) at 614-644-0701 or toll free at 800-644-0701.
   - Notify the Ohio State Highway Patrol.

   If there is clear and imminent danger and the agency Chief Legal Counsel is not available, the DPPOC can also contact the Ohio State Highway Patrol at 1-877-772-8765.

h. The office manager involved is responsible for notifying all individuals affected by CPI upon a finding that notification is required or prudent.

i. Employees and contractors should avoid reporting a suspected incident of access to CPI for an invalid reason to those parties suspected of performing or ordering such access.

j. Although employees are reminded of their duty to comply with the whistleblower statutes ORC 124.341 and ORC 4113.52, employees who report an access of CPI that they believe is for an invalid reason should have a reasonable factual basis for believing that improper activities have occurred. They should provide as much specific information as possible to allow for proper assessment of the nature, extent, and urgency of the incident.

V. REQUESTS FOR INCIDENT INFORMATION

If an OHFA employee or contractor receives a request for incident information directly from the public, or from any other individual who is not associated with the incident resolution, the OHFA employee or contractor will provide no information and will direct the request to the Chief Legal Counsel to follow the public records request policy.

VI. TRAINING

A review of this procedure will be included in regularly occurring OHFA training sessions. In addition, new employees must receive training on this standard operating procedure prior to accessing any OHFA system that contains CPI.

VII. MAINTENANCE OF THIS PROCEDURE

This procedure will be reviewed at least once annually to ensure it remains compliant with ORC 1347.15 and with any corresponding OHFA policy.

VIII.TABLE OF REVIEW DATES AND EFFECTIVE CHANGES

Date	Description
01/31/2021	New standard operating procedure

OHIO **HOUSING** FINANCE AGENCY

OHFA Log of Access to Confidential Personal Information

Name of Personal Information System: _____ Name of Employee with Access to CPI: _____

Acknowledgement: I acknowledge that the information on this log is true and complete and that (check one):

☐ I have accessed CPI only for purposes relating to my job duties or my agency's governmental function.

☐ I have not knowingly accessed CPI or directed access to CPI that would be logged under the OHFA procedure for Logging Access to Confidential Personal Information during the following monthly periods: (month/day/year) ____/____/_____ to ____/____/_____.

Initials: _____ Date of Acknowledgement: _____

Check here if this access log contains confidential information:

	Name (or identifier) of person whose CPI was accessed	Name of senior official or staff directing employee to access CPI (if applicable)	Reason for Access	Date access occurred (MM-DD-YYYY)	Time access occurred (hours and minutes)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					

USE OF INTERNET, E-MAIL AND OTHER IT RESOURCES (C7)

I. PURPOSE

This policy establishes controls on the use of state-provided information technology (IT) resources to ensure that they are appropriately used for the purposes for which they were acquired.

II. RELATED LAWS, RULES, POLICIES, REQUIREMENTS OR STANDARDS

- Computer Use Policy (C1)
- Policy on Protecting Privacy (C6)
- Policy on Discipline (A35)

III. APPLICABILITY

This policy applies to all OHFA employees, contractors, temporary personnel and others who have been granted access by the Agency to the state e-mail system and/or Agency-supplied internet and network services.

IV. DEFINITIONS

Availability - Ensuring timely and reliable access to and use of information.

Blog - Web-based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top. Blog topics can range from personal diaries to political issues, media programs and industry analysis. Blogs are also known as "Weblogs" or "Web logs."

Chat Room - An online forum where people can broadcast messages to people connected to the same forum in real time. Sometimes, these forums support audio and video communications, allowing people to converse and to see each other.

Cloud File Sharing Solutions - Cloud services that allow users to store and synchronize documents, photos, videos and other files in the cloud—and share them with other people. These services also allow users to share and synchronize data among multiple devices for a single owner. These services are accessible through desktops, notebooks, smartphones and media tablets, and provide a simple mechanism for synchronizing data across multiple devices.

Confidentiality - Preserving authorized restrictions on information access and disclosure, -including means for protecting personal privacy and proprietary information.

Confidential Personal Information (CPI) – PII that falls within the scope of section 1347.15 of the Revised Code and that OHFA is prohibited from releasing under Ohio's public records law.

Data - Coded representation of quantities, objects and actions. The word, "data," is often used interchangeably with the word, "information," in common usage and in this policy.

eDiscovery - "Discovery" refers to the process of complying with legal obligations to produce relevant documents and information to opposing counsel in the course of civil litigation or to prosecutors or government investigators in criminal or regulatory proceedings. "eDiscovery" refers to the production of files or other data held in an electronic form, such as e-mail.

Removable Media – Any portable device that is capable of storing information. Media is not required to be capable of processing information.

This definition includes, but is not limited to, the following:

- Diskettes
- External/removable hard drives
- Flash memory (e.g., secure digital (SD), Compact Flash, secure digital high capacity (SDHC), solid state drives, memory sticks)
- Magnetic tapes
- Portable Devices
- Optical media such as compact disks (CDs), digital video disks (DVDs), etc.
- Thumb drives (USB keys)/jump drives

Information Technology (IT) Resources - Any information technology resource, such as computer hardware and software, IT services, telecommunications equipment and services, digital devices such as digital copiers and facsimile machines, supplies and the Internet, made available to employees, contractors, temporary personnel and other agents of the state in the course of conducting state government business in support of agency mission and goals.

Instant Messaging - A software tool that allows real-time electronic messaging or chatting. Instant messaging services use "presence awareness," indicating whether people on one's list of contacts are currently online and available to chat.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Internet - A worldwide system of computer networks — a network of networks — in which computer users can get information and access services from other computers. The Internet is generally considered to be public, untrusted and outside the boundary of the state of Ohio enterprise network.

Listserv - An electronic mailing list software application that was originally developed in the 1980s and is also known as "discussion lists." A listserv subscriber uses the listserv to send messages to all the other subscribers, who may answer in similar fashion.

Malicious Code - Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Some examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Online Forum - A Web application where people post messages on specific topics. Forums are also known as Web forums, message boards, discussion boards and discussion groups.

Peer-to-Peer (P2P) File Sharing - Directly sharing content like audio, video, data, software or anything in digital format between any two computers connected to the network without the need for a central server.

Personally Identifiable Information (PII) - "Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics

Privileged User Accounts - Passwords associated with user accounts, which are assigned to individuals (commonly referend to as named accounts), that have elevated access to make changes to system parameters.

Save Password Option - An option on some systems that, when enabled, allows the user the choice of whether to have the user password memorized by the system so that it will not need to be re-entered upon subsequent access.

Secure FTP - A file transfer method that uses a Secure Shell or SSH network protocol to exchange data over a secure channel.

Sensitive Data - Sensitive data is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. The data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

Social Networks - Websites promoting a "circle of friends" or "virtual communities" where participants are connected based on various social commonalities such as familial bonds, hobbies or dating interests.

Telephone Service - Unless otherwise stated, telephone service includes both wired telephones and wireless telephones.

Wireless - Use of various electromagnetic spectrum frequencies, such as radio and infrared, to communicate services, such as data and voice, without relying on a hardwired connection, such as twisted pair, coaxial or fiber optic cable.

V. POLICY

It is the policy of OHFA to set standards on the use of the state e-mail system and/or Agency supplied internet, network services and other IT resources by employees, contractors, temporary personnel and others who may be granted access by the Agency.

1. **Use of Agency-provided IT resources**: The Agency provides computers, services, software, supplies and other IT resources to employees, contractors, temporary personnel and other agents of the state for supporting the work and conducting the affairs of OHFA. Personal use, if permitted as described in this policy, shall be strictly limited and can be restricted or revoked at the Agency's discretion at any time.

    1.1. Use of Agency-provided telephones and services: Restrictions on the use of IT resources outlined in this policy apply to wired and wireless telephone devices and services, including facsimile machines connected to the state's telephone service.

2. **Unacceptable Personal Use**: Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the state, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but is not limited to, the following:

    2.1. Violation of Law: Violating or supporting and encouraging the violation of local, state or federal law.

    2.2. Illegal Copying: Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws.

2.3. Operating a Business: Operating a business, directly or indirectly, for personal gain.

2.4. Accessing Personals Services: Accessing or participating in any type of personals advertisements or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personals advertisements.

2.5. Accessing Sexually Explicit Material: Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material.

2.6. Harassment: Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing.

2.7. Gambling or Wagering: Organizing, wagering on, participating in or observing any type of gambling event or activity.

2.8. Mass E-mailing: Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside of the state environment.

2.9. Solicitation: Except for Agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes.

3. **Participation in Online Communities**: Any use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, online forums, chat rooms, instant messaging, listservs, blogs, wikis, and social networks, is strictly prohibited unless organized by the Agency or approved by the employee's supervisor or the office director. Use of peer-to-peer file-sharing must be approved by the IT Office in addition to the supervisor or office director. If an individual is approved to participate in any of these forms of communication as part of Agency business, that person shall fulfill Agency-defined security education and awareness requirements for proper use before participating. The content of the education and awareness requirements shall include applicable office procedures and Agency-wide methods to avoid 1) inadvertent disclosure of sensitive information and 2) practices that could harm the security of state computer systems and networks, among other topics.

4. **Use of Cloud File Sharing Solutions**: Use of cloud file sharing solutions to store, share and synchronize state data must be approved by the employee's supervisor or the office director and the IT Office. The purpose of this requirement is to prohibit the use of cloud file sharing solutions that may not be adequately secured and that may compromise the Agency's ability to preserve and access information and comply with public records laws.

   When using Agency approved cloud file sharing solutions, the following restrictions apply:

   4.1. Cloud File Sharing and Data: Only data related to state business shall be stored in Agency approved cloud file sharing solutions.

   4.2. Sensitive Data and Cloud File Sharing Solutions: Cloud file sharing solutions are prohibited for the sharing of sensitive data. The Agency standard for sensitive data sharing is Secure FTP. Sensitive state data shall not be downloaded from cloud file sharing solutions onto personal devices.

5. **Unauthorized Installation or Use of Software**: Installing or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally owned software, without proper agency approval is strictly prohibited. Installation and use of unlicensed software is strictly prohibited.

6. **Unauthorized Installation or Use of Hardware**: Installing, attaching, or physically or wirelessly connecting any kind of hardware device (except for Bluetooth headphones, keyboards, and mice) to any Agency-provided IT resource, including computers and network services, without prior authorization is strictly prohibited. Connecting or attempting to connect a wireless device to the Agency's wireless service without proper Agency approval is strictly prohibited. Employees are permitted to connect personal devices, such as smart phones, to the Agency public Wi-Fi network but this is subject to change as needs warrant.

7. **No Expectation of Privacy**: This policy serves as notice to employees, contractors, temporary personnel and other agents of the state that they shall have no expectation of privacy in conjunction with their use of Agency-provided IT resources. Contents of Agency computers may be subject to review, investigation and public disclosure. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. The Agency reserves the right to view any files and electronic communications on state computers, monitor and log all electronic activities, and report findings to appropriate supervisors and authorities.

   7.1. Impeding Access: Impeding the Agency's ability to access, inspect and monitor IT resources is strictly prohibited. Employees, contractors, temporary personnel and other agents of the state shall not encrypt or conceal the contents of any file or electronic communication on Agency computers without proper authorization. Employees, contractors, temporary personnel and other agents of the state shall not set or manipulate a password on any Agency computer, program, file or electronic communication without proper authorization.

8. **Public Records**: Employees, contractors, temporary personnel and other agents of the state shall understand that records created as a result of the use of state provided IT resources may be subject to disclosure under Ohio's public records law and must be retained in accordance with state and Agency record retention schedules. In addition, the records created may also be subject to eDiscovery.
9. **Misrepresentation**: Concealing or misrepresenting one's name or affiliation to mask unauthorized, illegal, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.
10. **Restrictions on the Use of State E-mail Addresses**: Employees, contractors, temporary personnel and other agents of the state shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the state in the use of their assigned state e-mail address. State e-mail addresses shall not be used for personal communication in public forums such as, or similar to, listservs, discussion boards, discussion threads, comment forums, or blogs.
11. **Violations of Systems Security Measures**: Any use of Agency-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited.
    - 11.1. Confidentiality Procedures: Using IT resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.
    - 11.2. Accessing or Disseminating Sensitive Data or Personally Identifiable Information: Accessing or disseminating sensitive data or personally identifiable information, without authorization is strictly prohibited.
    - 11.3. Accessing Systems without Authorization: Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited. Employees, contractors, temporary personnel and other agents of the state are individually responsible for safeguarding their passwords.
    - 11.4. Duplicating Passwords: Employees, contractors, temporary personnel, and other agents of the state who are assigned both user accounts and privileged user accounts shall not use the same password for multiple accounts. Users must maintain unique passwords for each account.
    - 11.5. Save Password Option: Employees, contractors, temporary personnel, and other agents of the state shall not leverage save password options.
    - 11.6. Distributing Malicious Code: Distributing malicious code or circumventing malicious code security is strictly prohibited.
12. **Disciplinary Action**: Use of state Internet, email, and other IT resources, and compliance with state and federal law is a high priority of the Agency. Violations of this policy may constitute criminal offenses of theft, vandalism, or unauthorized use of property and may result in criminal and/or civil penalties, as well as be considered Misuse of State/OHFA Property and/or Insubordination pursuant to the Discipline Policy A-35 and the OCSEA Bargaining Unit Contract as appropriate.
13. **Contractual Agreements**: As of the effective date of this policy, any new contractual agreements for vendors and contractors shall include a requirement to comply with this policy as well as any associated Agency policies prior to gaining access to statewide and agency IT resources.

VI. MAINTENANCE OF THIS POLICY

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects OHFA PII and systems.

TABLE OF REVIEW DATE AND EFFECTIVE CHANGES

Number	Effective Date	Superseded/Modified	Significant Changes
C7	01/31/21	N/A	New Policy

DATA ENCRYPTION AND SECURING SENSITIVE DATA (C8)

I. PURPOSE

This policy in conjunction with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," establishes standards for the Agency to protect sensitive data and information.

II. RELATED LAWS, RULES, POLICIES, REQUIREMENTS OR STANDARDS

- Computer Use Policy (C1)
- Policy on Protecting Privacy (C6)
- IT-05 Disposal, Servicing and Transfer of IT Equipment
- IT-13, Data Classification
- ITS-SEC-01 Data Encryption and Cryptography
- ORC 125.18, 1347.12
- NIST SP 800-57, 800-88
- Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

III. APPLICABILITY

This policy applies to all OHFA employees, contractors, temporary personnel and others who gain access to the state e-mail system and/or Agency-supplied internet and network services.

IV. DEFINITIONS

Confidential Personal Information (CPI) –PII that falls within the scope of section 1347.15 of the Revised Code and that OHFA is prohibited from releasing under Ohio's public records law.

Encryption - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Information - Data processed into a form that has meaning and value to the recipient to support an action or decision. "Information" is often used interchangeably with "data" in common usage and in this policy.

Removable Media – Any portable device that is capable of storing information. Media is not required to be capable of processing information.

This definition includes, but is not limited to, the following:

- Diskettes
- External/removable hard drives
- Flash memory (e.g., secure digital (SD), Compact Flash, secure digital high capacity (SDHC), solid state drives, memory sticks)
- Magnetic tapes
- Portable Devices
- Optical media such as compact disks (CDs), digital video disks (DVDs), etc.
- Thumb drives (USB keys)/jump drives

Personally Identifiable Information (PII) - "Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics

Portable Devices - Computer or device designed for mobile use. For the purposes of this policy, a portable device includes laptops, smartphones or tablets.

Sensitive Data - Sensitive data is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. The data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

User - An individual or (system) process authorized to access an information system.

V. POLICY

Increased connectivity and mobility makes more data available to individuals, businesses and agencies. Consequently, sensitive information is more vulnerable to unauthorized disclosure, modification or destruction. Therefore, it is the policy of OHFA to implement the appropriate safeguards to protect sensitive data and information. This policy outlines the requirements for identifying and securing sensitive data as well as the devices and media on which sensitive data resides.

1. **Identify and Label Sensitive Data**: To help ensure that all sensitive data is protected, the Agency shall classify data, systems, media, devices and electronic transmissions in accordance with Ohio Administrative Policy IT-13, "Data Classification."
2. **Use Only State-Approved Strong Encryption**: Any use of encryption to protect sensitive data shall conform to Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography."
    2.1. The Agency shall ensure that a cryptographic key management plan is in place that protects the creation, distribution and storage of cryptographic keys as described by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57, Recommendations for Key Management Parts 1, 2 and 3.
3. **Secure Sensitive Data in Transmission**: The following methods shall be employed to secure sensitive data transmission:
    - Email: Sensitive data transmitted through email must be encrypted by using Zix™ in the Outlook client or setting the email sensitivity to "Confidential."
    - Secure FTP: FTP clients employed for the transmission of sensitive data must use a Secure Shell or SSH network protocol to exchange the data over a secure channel.
    - Secure Web Sites: Sensitive data may only be downloaded to or uploaded from websites using Transport Layer Security (HTTPS) encryption and user authentication.
    - Removable Media: Use of removable media to store sensitive data is prohibited. Sensitive data placed on media by external partners and sent to OHFA must be encrypted.

    The IT Office will check data in transmission for activities that risk unauthorized access to or disclosure of sensitive data via periodic review of activity logs.
4. **Secure Sensitive Data at Rest**: The Agency secures sensitive electronic data at rest through encryption. The following Agency practices are in place to secure access to sensitive data systems:
    4.1. Sensitive data may be downloaded only from Secure Web Sites and only when necessary to conduct Agency business;
    4.2. Individual access is limited through authorization controls to a need-to-know basis based on the user's role in the Agency;
    4.3. Devices providing access to sensitive data employ a session lock that requires re-authentication after 30 minutes or less of inactivity;
    4.4. The OHFA Help Desk implements a process for prompt deactivation of accounts for users who are no longer employed, shall no longer have access, or are subject to an action requiring deactivation; and
    4.5. A validation of user accounts to ensure that access rights are assigned appropriately shall be conducted periodically.
5. **Secure Backups**: In performing sensitive data backups and restorations, the Agency shall ensure:
    5.1. Encryption is consistently applied to backup devices, media and active data.
    5.2. Data backups enforce the most current access controls.
    5.3. Reuse of backup media is limited to the same set of sensitive data or is securely sanitized in accordance with NIST SP 800-88, "Guidelines for Media Sanitization," if it is used for another purpose.
    5.4. Backup media is destroyed in accordance with NIST SP 800-88 guidelines once it is no longer necessary.
    5.5. Appropriate physical security controls shall be in place, including:
        5.5.1. Physical access to backups of sensitive data shall be limited to authorized personnel only.
        5.5.2. Physical transportation of backup media shall be secure.
            - Transport shall be provided by a state employee or state approved secure carrier.
            - When possible, backup media shall be transported using a locked, tamper-proof box to secure the media.

5.5.3. Physical storage of sensitive data backups and restorations shall be located at an Agency-approved, secure facility.

6. **Sensitive Data on Portable Devices and Media**: Copying sensitive data onto portable devices and media, whether Agency-owned or personal, is prohibited.

   6.1. If portable devices or media are found to contain sensitive data, their removal or destruction along with the sensitive data shall be done in accordance with NIST SP 800-88 and the requirements outlined in Ohio Administrative Policy IT-05, "Disposal, Servicing and Transfer of IT Equipment."

7. **Physically Secure Sensitive Data**: The Agency shall secure the physical devices, locations and facilities used for sensitive data processing and storage.

   7.1. Only authorized personnel shall be allowed to access or remove devices and media containing sensitive data.

   7.2. In no event shall unencrypted sensitive data be stored or transported in a manner that is not physically secure. For unencrypted sensitive data, "physically secure" means implementing multiple layers of physical security that use facilities and services designed for securing high-risk data and certifying that the facilities or services take the necessary physical security precautions.

8. **Communicate Expectations for Handling Sensitive Data**: It is the user's responsibility to understand all the requirements associated with the protection of sensitive data as follows:

   8.1. Everyone has a duty to protect sensitive data;

   8.2. Sensitive data shall not be disclosed without authorization;

   8.3. Access to sensitive data shall not be provided without proper authorization;

   8.4. Sensitive data shall not be stored on devices that are personally-owned or otherwise not controlled by the Agency;

   8.5. There is no expectation of privacy when using state devices. The state has the right to access, inspect and monitor any state device or service including any files on or communications through state devices or services;

   8.6. In support of an investigation, the state may gain access to, or take custody of, non-state devices or services upon which the user has or appears to have placed state data; and

   8.7. Users who fail to adhere to these requirements are subject to the Discipline Policy A-35 and the OCSEA Bargaining Unit Contract as appropriate.

9. **Response to a Security Incident**: Compromise or exposure of sensitive data is addressed by the Agency incident response procedure, "Incident Response for Access of Confidential Personal Information for an Invalid Reason."

VI. ATTACHMENTS

Incident Response for Access of Confidential Personal Information for an Invalid Reason Procedure

VII. MAINTENANCE OF THIS POLICY

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects OHFA PII and systems.

TABLE OF REVIEW DATE AND EFFECTIVE CHANGES

Number	Effective Date	Superseded/Modified	Significant Changes
C8	01/31/21	N/A	New Policy

CLEAN DESK POLICY (F18)

I. PURPOSE

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/ critical information about our employees, our customers and our vendors is secure in locked areas and out of site. A Clean Desk Policy is part of standard basic privacy controls. A Clean Desk Policy helps to ensure that all sensitive information is removed from a workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting Sensitive Information.

II. RELATED LAWS, RULES, PROCEDURES, REQUIREMENTS OR STANDARDS

- OAC 175-10 – Accessing Confidential Personal Information
- Policy on Protecting Privacy C6
- Sensitive Paper Document Handling Policy D6

III. APPLICABILITY

This policy applies to all OHFA employees, contractors, temporary personnel and others who are granted access to the OHFA physical facility or working from home, state e-mail system and/or Agency-supplied internet and network services.

IV. DEFINITIONS

Personally Identifiable Information (PII) - For the purposes of this policy, "PII" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

Sensitive Information – For the purposes of this policy, means all data that is PII and Confidential Personal Information.

Confidential Personal Information (CPI) - PII that falls within the scope of section 1347.15 of the Ohio Revised Code and that OHFA is prohibited from releasing under Ohio Revised Code Section 175.12 pursuant to Ohio's public records law.

De-identification – A general term for any process of removing the association between a set of identifying data and the data subject.

Removable Media - Any portable device that is capable of storing information. Media is not required to be capable of processing information.

V. POLICY

It is the policy of OHFA to utilize all of the practices and processes to protect Sensitive Information from unauthorized access and to ensure Sensitive Information is only accessed by authorized individuals or parties.

VI. PROCEDURES

All employees and contract employees, contractors, temporary personnel and others who gain access to the OHFA facility or email or computer systems should do the following:

- Use De-identification of Sensitive Information whenever possible.
- Ensure that all Sensitive Information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be restarted at the end of the work day.
- Sensitive Information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- All file rooms and file cabinets containing Sensitive Information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Sensitive Information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

- Printouts containing Sensitive Information should be immediately removed from the printer.
- All documents containing Sensitive Information are to be shredded after use. Security containers are located on each floor at OHFA and are generally located near printing and copying stations. Security container contents are collected and shredded at scheduled intervals. (See Sensitive Paper Document Handling Policy (D6)).
- Whiteboards containing Sensitive Information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Use of removable media to store or transfer sensitive data is prohibited. Sensitive data placed on media by external partners and sent to OHFA must be encrypted
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that documents containing Sensitive Information are not left in printer trays for the wrong person to pick up.

VII. COMPLIANCE

OHFA management will verify compliance to this policy through various random methods including but not limited to, periodic walk-throughs, internal and external audits and feedback. Exceptions to the policy must be approved by the Executive Director or his/her designee in advance. Non-compliance to this policy may be subject to the Discipline Policy A-35 and the OCSEA Bargaining Unit Contract as appropriate.

VIII. MAINTENANCE OF THIS POLICY

This policy will be reviewed at least once annually to ensure that it remains compliant with Federal and State privacy laws including ORC Section 1347.15 and that it accurately reflects OHFA PII and systems.

TABLE OF EFFECTIVE CHANGES

Number	Effective Date	Superseded/Modified	Significant Changes
F18	01/31/21		New Policy