



## TELEWORK/REMOTE WORKSITE SELF-CERTIFICATION SAFETY CHECKLIST

Participating employees may use the following checklist to assist them in a survey of the overall safety and adequacy of their telework/remote worksite. The following are only recommendations and do not encompass every situation that may be encountered. Employees are encouraged to obtain professional assistance with issues concerning appropriate electrical service and circuit capacity for residential worksites.

- Practice a fire evacuation plan for use in the event of an emergency.
- Check your smoke detectors regularly and replace batteries once a year.
- Always have a working fire extinguisher conveniently located in your home and check the charge regularly.
- Computers can be heavy. Always place them on sturdy, level, well maintained furniture.
- Use a sturdy chair that provides good support and can be adjusted.
- Choose office chairs that provide good supporting backrests and allow adjustments to fit you comfortably.
- Locate your computer to eliminate noticeable glare from windows and lighting. Place computer monitor at height that is comfortable and does not require neck or back strain. Locate computer keyboards at heights that do not require wrist strain or place the keyboard on an adjustable surface.
- Install sufficient lighting in locations that reduce glare at the work surface.
- Arrange file cabinets so that open drawers do not block aisles.
- Be sure to leave aisle space where possible to reduce tripping hazards.
- Always make sure electrical equipment is connected to grounded outlets.
- Avoid fire hazards by never overloading electrical circuits.
- Inspect and repair carpeting with frayed edges or loose seams. Avoid using throw rugs that can cause tripping hazards in your workspace.
- Locate computers, phones and other electrical equipment in a manner that keeps power cords out of walkways.
- Power down computers after the workday is over and always turn off all electrical equipment during thunderstorms.
- Keep your work area clean and avoid clutter, which can cause fire and tripping hazards.
- Do not allow non-government employees to operate or repair government owned equipment.
- Always keep government files and information in a secure place and do not advertise your home office to strangers.
- Always use proper lifting techniques when moving or lifting heavy equipment and furniture.
- Always report accidents and injuries immediately to your supervisor.

## RULES OF BEHAVIOR FOR REMOTE ACCESS

### ***What is the Purpose of the Remote Access Rules of Behavior?***

The intent of these HUD Remote Access Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Program Offices as a basis for their own security plans.

### ***What are Rules of Behavior?***

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish

standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

### ***Who is Covered by These Rules?***

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

### ***What is Sensitive Data?***

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

### ***What are the Penalties for Non-Compliance?***

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the HUD published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

### ***Remote Access Users:***

- Users must adhere to the HUD Standards of Conduct and behave in an ethical, informed, and trustworthy manner.
- Users will complete annual HUD Information Technology Security Awareness training. Individuals identified as having significant information privacy responsibilities must take Privacy Act training. Contact your Information System Security Officer (ISSO) for details and availability.
- Use only systems, software, and data for which you have authorization and use them only for official government business, in accordance with the most current version of the U.S. Department of Housing and Urban Development Information Technology Security Policy, Handbook 2400.25 (to be referred to as the IT Security Handbook)
- Do not attempt to override technical or management controls (i.e., sensitive data should not be downloaded to any media or removed from HUD control without prior approval, etc.).
- Take precautions to secure government information and information resources. Protect government property, including hard copy documents, from theft, destruction, or misuse.
- Properly safeguard and dispose of media (both hardcopy and electronic) using approved means of destruction in accordance with applicable records management regulations and policies. Contact your ISSO for specific instructions.
- Physically protect laptop computers from theft through the use of locking devices whenever they are not attended. Be particularly aware of the threat of loss during periods of travel.
- Utilize and store sensitive data only on HUD-approved systems or devices.
- Do not copy government information onto personally owned equipment to include personal computers, external hard drives, portable "flash drives", or media players.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect personally identifiable information to ensure that it is not disclosed to unauthorized persons, either intentionally or unintentionally and abide by the most current HUD IT Security Handbook to safeguard information.
- Use or access sensitive data outside of HUD facilities only with prior approval from your supervisor.
- Use only authorized licensed HUD software on government equipment unless authorized to do so.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up to date.
- Change passwords frequently.

- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.
- Immediately report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials. Immediately report incidents in which sensitive information has been potentially lost or compromised to the HUD HITS Help Desk. (At the time of this form's issuance, for items involving phishing, contact Phishing@hud.gov; for IT security incidents, contact CIRT@hud.gov). For example, if you lose a cell phone, laptop, removable or external hard drive, flash drive, or hardcopy documentation that contains HUD information, it should be reported without delay. Refer to the HUD IT Security Policy for additional guidance on protecting sensitive data.

**Managers:**

- Ensure that staff is given access to, and ample time to complete, the annual HUD Information Security Awareness Training.
- Should review remote access authorizations annually to ensure that a bona fide business need exists.
- Ensure that personnel granted remote access follow established HUD IT security policies, guidelines and procedures.

**Specific Privacy Act Requirements:**

- Information systems containing personally identifiable information (e.g., SSN, name, photo, and address) must be protected and may be covered by a Privacy Act System of Records (SOR) Notice. This information will have added security controls you must follow.

For more information, review the [IT Security Handbook](#)

**EMPLOYEE CERTIFICATION:** I certify all information on this application and additional forms are true and correct. I understand and agree to abide by all of the requirements of the Flexiplace Policy as well as the requirements set forth in this document and, for bargaining unit employees, in any negotiated agreements related to the Flexiplace Program. Failure to do so may result in termination from the Flexiplace Program in accordance with the HUD Flexiplace Policy and any applicable negotiated agreements. Where the policy and an applicable negotiated agreement conflict, the negotiated agreement will prevail. I understand that violation of the Rules of Behavior for Remote Access could result in punishment and/or criminal prosecution. I certify that I have read the recommendations listed in the Self Certification Safety Checklist and I understand the elements and importance of safety at my alternative worksite. Further, I understand that flexiplace arrangements are not an entitlement and this agreement may be modified or terminated at any time. I certify that I have uploaded my required training certificate or that I am an AFGE employee who completed required telework training when I previously had an approved HUD telework agreement in place.

\_\_\_\_\_  
 Employee Signature 5/25/2022  
Date

**APPROVING OFFICIAL:** I certify the rules set forth in the Flexiplace Policy will be enforced. Additionally, I am aware of the compensatory and overtime provisions in the Policy. Approval is contingent upon the employee meeting all technological requirements and needs. If this is a remote work request that is being approved, I have obtained this decision from the Assistant Secretary or designee.

APPROVED  DISAPPROVED

DocuSigned by:  
 Cynthia Loesch-Johnson  
 \_\_\_\_\_  
 Supervisor Signature 5/26/2022  
Date

Title: Associate Regional Counsel for Housing Finance and Programs

**Reason if disapproved: Use the overflow box on the last page if more space is needed.**


Your position is not approved as a remote work eligible position at this time. Should the determination for your position change, you will be informed.

### FLEXIPLACE PROGRAM COORDINATOR

I certify I have reviewed this application in its entirety and all sections are complete, properly signed and all required forms are attached.

dara.a.powell@hud.gov

**FLEXIPLACE COORDINATOR E-MAIL ADDRESS**

**SIGNATURE:**  **DATE:** 6/3/2022

### ATTACHMENTS

**Training Certificate:** Please upload your Telework Fundamentals training certificate here before submitting this application. If you are an AFGE bargaining unit employee and you previously had an approved HUD telework agreement in place for which you completed required training in the past, then you do not need to upload anything.

The Telework Fundamentals training currently consists of five lessons, each of which offers a lesson completion certificate. Please ensure that you upload the *final completion certificate for the entire course*, which contains no red text referring to lesson numbers. The final course completion certificate is available only after you have completed all five lessons.

**Additional Supporting Documents:** Please feel free to add additional supporting documents as needed, but do not upload any medical documents. **Supervisors:** If you add any attachments, please discuss them with your employee first.

Click the paperclip icon below to add attachments.

Employee  
click to  
attach  
certificate  
or documents

First Line  
Supervisor  
click to  
attach  
documents



**Additional space for Type of Work to be Performed at ALTERNATIVE Worksite:**

**Additional space for Reason for Disapproval:**

**Privacy Notice:** The information collected on this form is needed for registering and approving individuals for participation in the HUD Flexiplace Program (telework and remote work). The results from collecting this information are used to conduct audits; respond to inquiries and/or investigations as required by legal authority; and to report on aggregate data within HUD, as well as to Congress (not personally identifiable information). Personally identifiable information is protected by applicable Federal laws, including but not limited to the Privacy Act of 1974, as amended (5 U.S. Code 552a)(e)(3); the Paperwork Reduction Act of 1995; the Freedom of Information Act; and the Telework Enhancement Act of 2010, Public Law 111–292.



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
WASHINGTON, DC 20410-0500

OFFICE OF THE GENERAL COUNSEL

May 18, 2022

FROM: Cynthia Loesch-Johnson, Associate Regional Counsel for Programs, 1AC

TO:

SUBJECT: Flexiplace Eligibility: Routine Telework

Dear \_\_\_\_\_,

We are excited to move HUD forward under the new Flexiplace Program, which provides expanded options for workplace flexibilities. Upon completion of an initial assessment of the positions within our program office, we have determined that your position is eligible for the option of: routine telework. This is the maximum flexibility your position is eligible for at this time. We will continue to assess our business needs and functions of positions on an ongoing basis to determine if a different level of flexibility should be authorized in the future.

Participation in telework is voluntary. Under routine telework you are required to report to an approved HUD office at least twice a pay period regardless of your work schedule type. The number of telework days you will be approved for is subject to supervisory approval.

If your telework application is approved for routine telework, the approval automatically includes situational telework. Under situational telework you may request approval to use situational telework on an occasional, as needed basis. Alternatively, you may request to only participate in telework situationally and not on a regular and recurring basis.

If you are interested in teleworking, please apply via the HUD-25228 Flexiplace Application & Agreement form, routed through DocuSign, which you can access later this pay period via the Flexiplace Information Center page on HUD@Work. Even if you have an existing telework agreement that you would like to keep the same, please document this arrangement by completing the form in DocuSign.

### **Workspace in the HUD Office**

Please keep in mind that in the future, those employees reporting to a HUD office 6 or more days per pay period will be entitled to a dedicated office space, but those reporting to a HUD office 5 or fewer days a pay period may need to participate in a shared workspace arrangement like hoteling or hot desking. This will be implemented incrementally in most locations and after completing negotiations with our Union partners.

Please refer to the Flexiplace Information Center page for more information.  
Thank you for your support as we work together to continue to move HUD Forward.

# FLEXIPLACE APPLICATION & AGREEMENT

EMPLOYEE NAME	Portfolio Management Specialist, GS1101-13
PIH	amabelle.aponte@hud.gov
PROGRAM OFFICE	IMMEDIATE SUPERVISOR E-MAIL ADDRESS
OFFICE PHONE NUMBER	CURRENT OFFICIAL DUTY STATION ADDRESS
	235 Federico St, Suite 200, San Juan, PR 00918

## TELEWORK OR REMOTE WORKSITE

ADDRESS: \_\_\_\_\_ TELEPHONE NUMBER: \_\_\_\_\_

CITY: \_\_\_\_\_ COUNTY: \_\_\_\_\_ STATE: \_\_\_\_\_

## TYPE OF FLEXIPLACE ARRANGEMENT

**REGULAR TELEWORK - Number of days per pay period \_\_\_\_\_**

**NOTE:** If you select Regular Telework, you are automatically approved for Situational Telework.

**SITUATIONAL TELEWORK ONLY**       **COOP TELEWORK ONLY**

**NOTE:** If this application is being submitted in order to utilize only Situational or COOP telework in the future, employees must provide start and end dates and a reason/justification by email to the approving official each time telework is to be used and obtain approval in writing.

**REMOTE WORK – NEAR HUD OFFICE (within 50 miles of HUD office)**

**REMOTE WORK – OUTSIDE COMMUTING AREA (more than 50 miles from HUD office)**

## TOUR OF DUTY

**NOTE:** For employees on flexitime/flexitour schedules, start times may vary from those indicated within the applicable window.

Work Week 1	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site		Work Week 2	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site
Monday	8:00am	4:30pm	TW/Remote		Monday	8:00am	4:30pm	TW/Remote
Tuesday	8:00am	4:30pm	TW/Remote		Tuesday	8:00am	4:30pm	TW/Remote
Wednesday	8:00am	4:30pm	TW/Remote		Wednesday	8:00am	4:30pm	TW/Remote
Thursday	8:00am	4:30pm	TW/Remote		Thursday	8:00am	4:30pm	TW/Remote
Friday	8:00am	4:30pm	TW/Remote		Friday	8:00am	4:30pm	TW/Remote

Identify type of work to be performed at ALTERNATIVE/REMOTE worksite. Use the overflow box on the last page if more space is needed.

All work/duties OR identify specific tasks below:

EMPLOYEE AGREES TO RETRIEVE VOICE MAIL MESSAGES EVERY \_\_\_\_\_ HOURS AND TO RESPOND WITHIN \_\_\_\_\_ HOURS OR

EMPLOYEE WILL USE CALL FORWARDING FROM A HUD PHONE NUMBER OR USE A HUD-ISSUED CELL PHONE

Other Requirements: \_\_\_\_\_

## TECHNOLOGICAL INFORMATION

I have internet access at my alternative/remote worksite.     High Speed     Other (Explain): \_\_\_\_\_

I have a HUD-issued laptop.

I use a personal computer at my alternative/remote worksite in accordance with IT Helpdesk instructions because a HUD laptop is not available.



## TELEWORK/REMOTE WORKSITE SELF-CERTIFICATION SAFETY CHECKLIST

Participating employees may use the following checklist to assist them in a survey of the overall safety and adequacy of their telework/remote worksite. The following are only recommendations and do not encompass every situation that may be encountered. Employees are encouraged to obtain professional assistance with issues concerning appropriate electrical service and circuit capacity for residential worksites.

- Practice a fire evacuation plan for use in the event of an emergency.
- Check your smoke detectors regularly and replace batteries once a year.
- Always have a working fire extinguisher conveniently located in your home and check the charge regularly.
- Computers can be heavy. Always place them on sturdy, level, well maintained furniture.
- Use a sturdy chair that provides good support and can be adjusted.
- Choose office chairs that provide good supporting backrests and allow adjustments to fit you comfortably.
- Locate your computer to eliminate noticeable glare from windows and lighting. Place computer monitor at height that is comfortable and does not require neck or back strain. Locate computer keyboards at heights that do not require wrist strain or place the keyboard on an adjustable surface.
- Install sufficient lighting in locations that reduce glare at the work surface.
- Arrange file cabinets so that open drawers do not block aisles.
- Be sure to leave aisle space where possible to reduce tripping hazards.
- Always make sure electrical equipment is connected to grounded outlets.
- Avoid fire hazards by never overloading electrical circuits.
- Inspect and repair carpeting with frayed edges or loose seams. Avoid using throw rugs that can cause tripping hazards in your workspace.
- Locate computers, phones and other electrical equipment in a manner that keeps power cords out of walkways.
- Power down computers after the workday is over and always turn off all electrical equipment during thunderstorms.
- Keep your work area clean and avoid clutter, which can cause fire and tripping hazards.
- Do not allow non-government employees to operate or repair government owned equipment.
- Always keep government files and information in a secure place and do not advertise your home office to strangers.
- Always use proper lifting techniques when moving or lifting heavy equipment and furniture.
- Always report accidents and injuries immediately to your supervisor.

## RULES OF BEHAVIOR FOR REMOTE ACCESS

### ***What is the Purpose of the Remote Access Rules of Behavior?***

The intent of these HUD Remote Access Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Program Offices as a basis for their own security plans.

### ***What are Rules of Behavior?***

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish

standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

### ***Who is Covered by These Rules?***

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

### ***What is Sensitive Data?***

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

### ***What are the Penalties for Non-Compliance?***

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the HUD published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

### ***Remote Access Users:***

- Users must adhere to the HUD Standards of Conduct and behave in an ethical, informed, and trustworthy manner.
- Users will complete annual HUD Information Technology Security Awareness training. Individuals identified as having significant information privacy responsibilities must take Privacy Act training. Contact your Information System Security Officer (ISSO) for details and availability.
- Use only systems, software, and data for which you have authorization and use them only for official government business, in accordance with the most current version of the U.S. Department of Housing and Urban Development Information Technology Security Policy, Handbook 2400.25 (to be referred to as the IT Security Handbook)
- Do not attempt to override technical or management controls (i.e., sensitive data should not be downloaded to any media or removed from HUD control without prior approval, etc.).
- Take precautions to secure government information and information resources. Protect government property, including hard copy documents, from theft, destruction, or misuse.
- Properly safeguard and dispose of media (both hardcopy and electronic) using approved means of destruction in accordance with applicable records management regulations and policies. Contact your ISSO for specific instructions.
- Physically protect laptop computers from theft through the use of locking devices whenever they are not attended. Be particularly aware of the threat of loss during periods of travel.
- Utilize and store sensitive data only on HUD-approved systems or devices.
- Do not copy government information onto personally owned equipment to include personal computers, external hard drives, portable "flash drives", or media players.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect personally identifiable information to ensure that it is not disclosed to unauthorized persons, either intentionally or unintentionally and abide by the most current HUD IT Security Handbook to safeguard information.
- Use or access sensitive data outside of HUD facilities only with prior approval from your supervisor.
- Use only authorized licensed HUD software on government equipment unless authorized to do so.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up to date.
- Change passwords frequently.

- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.
- Immediately report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials. Immediately report incidents in which sensitive information has been potentially lost or compromised to the HUD HITS Help Desk. (At the time of this form's issuance, for items involving phishing, contact Phishing@hud.gov; for IT security incidents, contact CIRT@hud.gov). For example, if you lose a cell phone, laptop, removable or external hard drive, flash drive, or hardcopy documentation that contains HUD information, it should be reported without delay. Refer to the HUD IT Security Policy for additional guidance on protecting sensitive data.

**Managers:**

- Ensure that staff is given access to, and ample time to complete, the annual HUD Information Security Awareness Training.
- Should review remote access authorizations annually to ensure that a bona fide business need exists.
- Ensure that personnel granted remote access follow established HUD IT security policies, guidelines and procedures.

**Specific Privacy Act Requirements:**

- Information systems containing personally identifiable information (e.g., SSN, name, photo, and address) must be protected and may be covered by a Privacy Act System of Records (SOR) Notice. This information will have added security controls you must follow.

For more information, review the [IT Security Handbook](#)

**EMPLOYEE CERTIFICATION:** I certify all information on this application and additional forms are true and correct. I understand and agree to abide by all of the requirements of the Flexiplace Policy as well as the requirements set forth in this document and, for bargaining unit employees, in any negotiated agreements related to the Flexiplace Program. Failure to do so may result in termination from the Flexiplace Program in accordance with the HUD Flexiplace Policy and any applicable negotiated agreements. Where the policy and an applicable negotiated agreement conflict, the negotiated agreement will prevail. I understand that violation of the Rules of Behavior for Remote Access could result in punishment and/or criminal prosecution. I certify that I have read the recommendations listed in the Self Certification Safety Checklist and I understand the elements and importance of safety at my alternative worksite. Further, I understand that flexiplace arrangements are not an entitlement and this agreement may be modified or terminated at any time. I certify that I have uploaded my required training certificate or that I am an AFGE employee who completed required telework training when I previously had an approved HUD telework agreement in place.

DocuSigned by:  
 \_\_\_\_\_ 6/2/2022  
 Employee Signature Date

**APPROVING OFFICIAL:** I certify the rules set forth in the Flexiplace Policy will be enforced. Additionally, I am aware of the compensatory and overtime provisions in the Policy. Approval is contingent upon the employee meeting all technological requirements and needs. If this is a remote work request that is being approved, I have obtained this decision from the Assistant Secretary or designee.

DocuSigned by:  APPROVED  DISAPPROVED  
 \_\_\_\_\_ 6/6/2022  
 Supervisor Signature Date

Title: Division Director

**Reason if disapproved:** Use the overflow box on the last page if more space is needed.

See disapproval letter from the delegated official.

### FLEXIPLACE PROGRAM COORDINATOR

I certify I have reviewed this application in its entirety and all sections are complete, properly signed and all required forms are attached.

Emily.Montague@hud.gov

**FLEXIPLACE COORDINATOR E-MAIL ADDRESS**

**SIGNATURE:** \_\_\_\_\_ **DATE:** \_\_\_\_\_

### ATTACHMENTS

**Training Certificate:** Please upload your Telework Fundamentals training certificate here before submitting this application. If you are an AFGE bargaining unit employee and you previously had an approved HUD telework agreement in place for which you completed required training in the past, then you do not need to upload anything.

The Telework Fundamentals training currently consists of five lessons, each of which offers a lesson completion certificate. Please ensure that you upload the *final completion certificate for the entire course*, which contains no red text referring to lesson numbers. The final course completion certificate is available only after you have completed all five lessons.

**Additional Supporting Documents:** Please feel free to add additional supporting documents as needed, but do not upload any medical documents. **Supervisors:** If you add any attachments, please discuss them with your employee first.

Click the paperclip icon below to add attachments.

Employee  
click to  
attach  
certificate  
or documents

First Line  
Supervisor  
click to  
attach  
documents



**Additional space for Type of Work to be Performed at ALTERNATIVE Worksite:**

**Additional space for Reason for Disapproval:**

In Process

**Privacy Notice:** The information collected on this form is needed for registering and approving individuals for participation in the HUD Flexiplace Program (telework and remote work). The results from collecting this information are used to conduct audits; respond to inquiries and/or investigations as required by legal authority; and to report on aggregate data within HUD, as well as to Congress (not personally identifiable information). Personally identifiable information is protected by applicable Federal laws, including but not limited to the Privacy Act of 1974, as amended (5 U.S. Code 552a)(e)(3); the Paperwork Reduction Act of 1995; the Freedom of Information Act; and the Telework Enhancement Act of 2010, Public Law 111–292.



**June 2, 2022**

**Greetings PIH Flexiplace Remote Work Applicant:**

Thank you for submitting a Flexiplace application requesting to work on a remote basis.

The purpose of this memo is to inform you that **your position** was not approved as a remote work eligible position at this time. Therefore, your request to work on a remote basis cannot be approved. Should the Department's determination for your position change, you will be informed.

Since your Flexiplace application is being denied at this time, you may appeal the denial of the remote work request to the PIH Deputy Assistant Secretary (DAS) of Operations, by emailing your appeal to: [PIH-DASofOPS@hud.gov](mailto:PIH-DASofOPS@hud.gov). The **Subject Line** of the email should reference: **Flexiplace Remote Work Appeal – (and your name)**. Please note the following requirements for submitting an appeal.

- You must appeal the decision within **15 calendar days** of receipt of the denial.
- Your appeal must be accompanied by any circumstances you believe are relevant to the request for reconsideration.

The DAS of Operations will render a written decision **within 21 calendar days** from receipt of the appeal.

Please stay apprised of any future developments in the Flexiplace program.

Respectfully,

*Cedric A. Brown*

Cedric A. Brown  
Delegated Flexiplace Official for PIH  
Director, Office of Business Support  
HUD Office of Public & Indian Housing

**Certificate Of Completion**

Envelope Id: 90E93118307F490EBED9B8C8DF1A02F5	Status: Sent
Subject: Flexiplace Application for	
Source Envelope:	
Document Pages: 7	Signatures: 2
Certificate Pages: 5	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Return to Work Questions
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	451 7th Street NW
	Washington, DC 20410
	ReturntoWorkQuestions@hud.gov
	IP Address: 170.97.202.202

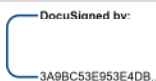
**Record Tracking**

Status: Original	Holder: Return to Work Questions	Location: DocuSign
6/2/2022 10:38:16 AM	ReturntoWorkQuestions@hud.gov	
Security Appliance Status: Connected	Pool: FedRamp	
Storage Appliance Status: Connected	Pool: Admin - Flexiplace	Location: DocuSign

**Signer Events**

Security Level:  
DocuSign.email  
ID: 1  
6/2/2022 10:38:19 AM

**Signature**

DocuSigned by:  
  
3A9BC53E953E4DB...

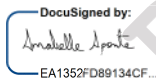
Signature Adoption: Pre-selected Style  
Signed by link sent to  
Using IP Address: 170.97.202.202

**Timestamp**

Sent: 6/2/2022 10:38:18 AM  
Viewed: 6/2/2022 10:38:33 AM  
Signed: 6/2/2022 11:20:22 AM

**Electronic Record and Signature Disclosure:**  
Accepted: 6/2/2022 10:36:50 AM  
ID: 23e8263a-6e19-4318-adcf-cbd977890ce3

Amabelle Aponte  
amabelle.aponte@hud.gov  
Security Level: Email, Account Authentication  
(None)

DocuSigned by:  
  
EA1352FD89134CF...

Signature Adoption: Pre-selected Style  
Signed by link sent to amabelle.aponte@hud.gov  
Using IP Address: 170.97.91.22

Sent: 6/2/2022 11:20:26 AM  
Viewed: 6/3/2022 10:00:40 AM  
Signed: 6/6/2022 8:04:52 AM

**Electronic Record and Signature Disclosure:**  
Accepted: 6/3/2022 10:00:40 AM  
ID: bf0d9bf3-6027-4427-9727-648e425d424b

Emily Montague  
Emily.Montague@hud.gov  
Security Level: Email, Account Authentication  
(None)

**Electronic Record and Signature Disclosure:**  
Accepted: 5/23/2022 11:12:22 AM  
ID: 7a70a2ec-b49c-4863-a11e-9603668fc35b

Sent: 6/6/2022 8:04:56 AM

**In Person Signer Events**

**Signature**

**Timestamp**

**Editor Delivery Events**

**Status**

**Timestamp**

**Agent Delivery Events**

**Status**

**Timestamp**

**Intermediary Delivery Events**

**Status**

**Timestamp**

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

**COPIED**

Sent: 6/2/2022 11:20:25 AM  
Viewed: 6/6/2022 8:47:10 AM

Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Amabelle Aponte

amabelle.aponte@hud.gov

Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Accepted: 6/3/2022 10:00:40 AM  
ID: bf0d9bf3-6027-4427-9727-648e425d424b

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	6/2/2022 10:38:18 AM
---------------	------------------	----------------------

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--

In PROCESS



## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Admin - Flexiplace (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact Admin - Flexiplace:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov)

### **To advise Admin - Flexiplace of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from Admin - Flexiplace**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with Admin - Flexiplace**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to DocuSignRequest@hud.gov and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Admin - Flexiplace as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Admin - Flexiplace during the course of your relationship with Admin - Flexiplace.

# FLEXIPLACE APPLICATION & AGREEMENT

EMPLOYEE NAME	Equal Opp. Specialist, 0360, GS-13
FHEO	emily.toxha@hud.gov
PROGRAM OFFICE	IMMEDIATE SUPERVISOR E-MAIL ADDRESS
OFFICE PHONE NUMBER	CURRENT OFFICIAL DUTY STATION ADDRESS
	10 Causeway Street #321, Boston, MA 02222

## TELEWORK OR REMOTE WORKSITE

ADDRESS: [REDACTED] TELEPHONE NUMBER: [REDACTED]

CITY: [REDACTED] COUNTY: [REDACTED] STATE: [REDACTED]

## TYPE OF FLEXIPLACE ARRANGEMENT

**REGULAR TELEWORK - Number of days per pay period \_\_\_\_\_**

**NOTE:** If you select Regular Telework, you are automatically approved for Situational Telework.

**SITUATIONAL TELEWORK ONLY**       **COOP TELEWORK ONLY**

**NOTE:** If this application is being submitted in order to utilize only Situational or COOP telework in the future, employees must provide start and end dates and a reason/justification by email to the approving official each time telework is to be used and obtain approval in writing.

**REMOTE WORK – NEAR HUD OFFICE (within 50 miles of HUD office)**

**REMOTE WORK – OUTSIDE COMMUTING AREA (more than 50 miles from HUD office)**

## TOUR OF DUTY

**NOTE:** For employees on flexitime/flexitour schedules, start times may vary from those indicated within the applicable window.

Work Week 1	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site		Work Week 2	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site
Monday	8:00	4:30	TW/Remote		Monday	8:00	4:30	TW/Remote
Tuesday	8:00	4:30	TW/Remote		Tuesday	8:00	4:30	TW/Remote
Wednesday	8:00	4:30	TW/Remote		Wednesday	8:00	4:30	TW/Remote
Thursday	8:00	4:30	TW/Remote		Thursday	8:00	4:30	TW/Remote
Friday	8:00	4:30	TW/Remote		Friday	8:00	4:30	TW/Remote

Identify type of work to be performed at ALTERNATIVE/REMOTE worksite. Use the overflow box on the last page if more space is needed.

**All work/duties OR identify specific tasks below:**

All work/duties including union representational duties, which may require visits to the union office and other Regional offices.

**EMPLOYEE AGREES TO RETRIEVE VOICE MAIL MESSAGES EVERY \_\_\_\_\_ HOURS AND TO RESPOND WITHIN \_\_\_\_\_ HOURS OR**

**EMPLOYEE WILL USE CALL FORWARDING FROM A HUD PHONE NUMBER OR USE A HUD-ISSUED CELL PHONE**

Other Requirements: \_\_\_\_\_

## TECHNOLOGICAL INFORMATION

**I have internet access at my alternative/remote worksite.**     **High Speed**     **Other (Explain): \_\_\_\_\_**

**I have a HUD-issued laptop.**

**I use a personal computer at my alternative/remote worksite in accordance with IT Helpdesk instructions because a HUD laptop is not available.**

## TELEWORK/REMOTE WORKSITE SELF-CERTIFICATION SAFETY CHECKLIST

Participating employees may use the following checklist to assist them in a survey of the overall safety and adequacy of their telework/remote worksite. The following are only recommendations and do not encompass every situation that may be encountered. Employees are encouraged to obtain professional assistance with issues concerning appropriate electrical service and circuit capacity for residential worksites.

- Practice a fire evacuation plan for use in the event of an emergency.
- Check your smoke detectors regularly and replace batteries once a year.
- Always have a working fire extinguisher conveniently located in your home and check the charge regularly.
- Computers can be heavy. Always place them on sturdy, level, well maintained furniture.
- Use a sturdy chair that provides good support and can be adjusted.
- Choose office chairs that provide good supporting backrests and allow adjustments to fit you comfortably.
- Locate your computer to eliminate noticeable glare from windows and lighting. Place computer monitor at height that is comfortable and does not require neck or back strain. Locate computer keyboards at heights that do not require wrist strain or place the keyboard on an adjustable surface.
- Install sufficient lighting in locations that reduce glare at the work surface.
- Arrange file cabinets so that open drawers do not block aisles.
- Be sure to leave aisle space where possible to reduce tripping hazards.
- Always make sure electrical equipment is connected to grounded outlets.
- Avoid fire hazards by never overloading electrical circuits.
- Inspect and repair carpeting with frayed edges or loose seams. Avoid using throw rugs that can cause tripping hazards in your workspace.
- Locate computers, phones and other electrical equipment in a manner that keeps power cords out of walkways.
- Power down computers after the workday is over and always turn off all electrical equipment during thunderstorms.
- Keep your work area clean and avoid clutter, which can cause fire and tripping hazards.
- Do not allow non-government employees to operate or repair government owned equipment.
- Always keep government files and information in a secure place and do not advertise your home office to strangers.
- Always use proper lifting techniques when moving or lifting heavy equipment and furniture.
- Always report accidents and injuries immediately to your supervisor.

## RULES OF BEHAVIOR FOR REMOTE ACCESS

### ***What is the Purpose of the Remote Access Rules of Behavior?***

The intent of these HUD Remote Access Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Program Offices as a basis for their own security plans.

### ***What are Rules of Behavior?***

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish

standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

### ***Who is Covered by These Rules?***

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

### ***What is Sensitive Data?***

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

### ***What are the Penalties for Non-Compliance?***

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the HUD published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

### ***Remote Access Users:***

- Users must adhere to the HUD Standards of Conduct and behave in an ethical, informed, and trustworthy manner.
- Users will complete annual HUD Information Technology Security Awareness training. Individuals identified as having significant information privacy responsibilities must take Privacy Act training. Contact your Information System Security Officer (ISSO) for details and availability.
- Use only systems, software, and data for which you have authorization and use them only for official government business, in accordance with the most current version of the U.S. Department of Housing and Urban Development Information Technology Security Policy, Handbook 2400.25 (to be referred to as the IT Security Handbook)
- Do not attempt to override technical or management controls (i.e., sensitive data should not be downloaded to any media or removed from HUD control without prior approval, etc.).
- Take precautions to secure government information and information resources. Protect government property, including hard copy documents, from theft, destruction, or misuse.
- Properly safeguard and dispose of media (both hardcopy and electronic) using approved means of destruction in accordance with applicable records management regulations and policies. Contact your ISSO for specific instructions.
- Physically protect laptop computers from theft through the use of locking devices whenever they are not attended. Be particularly aware of the threat of loss during periods of travel.
- Utilize and store sensitive data only on HUD-approved systems or devices.
- Do not copy government information onto personally owned equipment to include personal computers, external hard drives, portable "flash drives", or media players.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect personally identifiable information to ensure that it is not disclosed to unauthorized persons, either intentionally or unintentionally and abide by the most current HUD IT Security Handbook to safeguard information.
- Use or access sensitive data outside of HUD facilities only with prior approval from your supervisor.
- Use only authorized licensed HUD software on government equipment unless authorized to do so.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up to date.
- Change passwords frequently.

- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.
- Immediately report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials. Immediately report incidents in which sensitive information has been potentially lost or compromised to the HUD HITS Help Desk. (At the time of this form's issuance, for items involving phishing, contact Phishing@hud.gov; for IT security incidents, contact CIRT@hud.gov). For example, if you lose a cell phone, laptop, removable or external hard drive, flash drive, or hardcopy documentation that contains HUD information, it should be reported without delay. Refer to the HUD IT Security Policy for additional guidance on protecting sensitive data.

**Managers:**

- Ensure that staff is given access to, and ample time to complete, the annual HUD Information Security Awareness Training.
- Should review remote access authorizations annually to ensure that a bona fide business need exists.
- Ensure that personnel granted remote access follow established HUD IT security policies, guidelines and procedures.

**Specific Privacy Act Requirements:**

- Information systems containing personally identifiable information (e.g., SSN, name, photo, and address) must be protected and may be covered by a Privacy Act System of Records (SOR) Notice. This information will have added security controls you must follow.

For more information, review the [IT Security Handbook](#)

**EMPLOYEE CERTIFICATION:** I certify all information on this application and additional forms are true and correct. I understand and agree to abide by all of the requirements of the Flexiplace Policy as well as the requirements set forth in this document and, for bargaining unit employees, in any negotiated agreements related to the Flexiplace Program. Failure to do so may result in termination from the Flexiplace Program in accordance with the HUD Flexiplace Policy and any applicable negotiated agreements. Where the policy and an applicable negotiated agreement conflict, the negotiated agreement will prevail. I understand that violation of the Rules of Behavior for Remote Access could result in punishment and/or criminal prosecution. I certify that I have read the recommendations listed in the Self Certification Safety Checklist and I understand the elements and importance of safety at my alternative worksite. Further, I understand that flexiplace arrangements are not an entitlement and this agreement may be modified or terminated at any time. I certify that I have uploaded my required training certificate or that I am an AFGE employee who completed required telework training when I previously had an approved HUD telework agreement in place.

\_\_\_\_\_  
 Employee Signature 6/8/2022  
 \_\_\_\_\_  
Date

**APPROVING OFFICIAL:** I certify the rules set forth in the Flexiplace Policy will be enforced. Additionally, I am aware of the compensatory and overtime provisions in the Policy. Approval is contingent upon the employee meeting all technological requirements and needs. If this is a remote work request that is being approved, I have obtained this decision from the Assistant Secretary or designee.

APPROVED  DISAPPROVED

DocuSigned by:  
 Emily Loyha  
 \_\_\_\_\_  
 Supervisor Signature 6/8/2022  
 \_\_\_\_\_  
Date

Title: Enforcement Branch Chief

**Reason if disapproved:** Use the overflow box on the last page if more space is needed.  
 Flexi-place policy guidance.

### FLEXIPLACE PROGRAM COORDINATOR

I certify I have reviewed this application in its entirety and all sections are complete, properly signed and all required forms are attached.

angela.e.williams@hud.gov

**FLEXIPLACE COORDINATOR E-MAIL ADDRESS**

**SIGNATURE:** \_\_\_\_\_ **DATE:** \_\_\_\_\_

### ATTACHMENTS

**Training Certificate:** Please upload your Telework Fundamentals training certificate here before submitting this application. If you are an AFGE bargaining unit employee and you previously had an approved HUD telework agreement in place for which you completed required training in the past, then you do not need to upload anything.

The Telework Fundamentals training currently consists of five lessons, each of which offers a lesson completion certificate. Please ensure that you upload the *final completion certificate for the entire course*, which contains no red text referring to lesson numbers. The final course completion certificate is available only after you have completed all five lessons.

**Additional Supporting Documents:** Please feel free to add additional supporting documents as needed, but do not upload any medical documents. **Supervisors:** If you add any attachments, please discuss them with your employee first.

Click the paperclip icon below to add attachments.

Employee  
click to  
attach  
certificate  
or documents

First Line  
Supervisor  
click to  
attach  
documents





**Additional space for Type of Work to be Performed at ALTERNATIVE Worksite:**

**Additional space for Reason for Disapproval:**

In Process

**Privacy Notice:** The information collected on this form is needed for registering and approving individuals for participation in the HUD Flexiplace Program (telework and remote work). The results from collecting this information are used to conduct audits; respond to inquiries and/or investigations as required by legal authority; and to report on aggregate data within HUD, as well as to Congress (not personally identifiable information). Personally identifiable information is protected by applicable Federal laws, including but not limited to the Privacy Act of 1974, as amended (5 U.S. Code 552a)(e)(3); the Paperwork Reduction Act of 1995; the Freedom of Information Act; and the Telework Enhancement Act of 2010, Public Law 111–292.

**Certificate Of Completion**

Envelope Id: E6B903042CA54F89BA24DBFCB2562799	Status: Sent
Subject: Flexiplace Application for	
Source Envelope:	
Document Pages: 6	Signatures: 2
Certificate Pages: 5	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Return to Work Questions
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	451 7th Street NW
	Washington, DC 20410
	ReturntoWorkQuestions@hud.gov
	IP Address: 170.97.202.202

**Record Tracking**

Status: Original	Holder: Return to Work Questions	Location: DocuSign
6/8/2022 8:58:00 AM	ReturntoWorkQuestions@hud.gov	
Security Appliance Status: Connected	Pool: FedRamp	
Storage Appliance Status: Connected	Pool: Admin - Flexiplace	Location: DocuSign

**Signer Events**

Signature	Timestamp
	Sent: 6/8/2022 8:58:04 AM
	Viewed: 6/8/2022 8:58:16 AM
	Signed: 6/8/2022 9:01:55 AM
DocuSign.email ID: 1 6/8/2022 8:58:05 AM	Signature Adoption: Pre-selected Style Signed by link sent to Using IP Address: 170.97.202.202

**Electronic Record and Signature Disclosure:**  
Accepted: 5/19/2022 7:19:32 AM  
ID: 3b9785a1-0382-4fa5-8fb7-258e0577c23f

Emily Loxha  
emily.loxha@hud.gov  
x

DocuSigned by:  
*Emily Loxha*  
5EFBE43019F846E...

Sent: 6/8/2022 9:02:01 AM  
Viewed: 6/8/2022 9:02:57 AM  
Signed: 6/8/2022 9:03:18 AM

FHEO  
Security Level: Email, Account Authentication  
(None)

Signature Adoption: Pre-selected Style  
Signed by link sent to emily.loxha@hud.gov  
Using IP Address: 170.97.91.25

**Electronic Record and Signature Disclosure:**  
Accepted: 5/19/2022 7:39:10 AM  
ID: 996524f4-4178-41aa-a464-1472fa7606ce

Angela E. Williams  
angela.e.williams@hud.gov  
FHEO

Sent: 6/8/2022 9:03:21 AM

Security Level: Email, Account Authentication  
(None)

**Electronic Record and Signature Disclosure:**  
Accepted: 5/19/2022 8:22:59 AM  
ID: 90396c08-4c1a-4645-bee5-1e342b189286

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

**COPIED**

Sent: 6/8/2022 9:02:00 AM  
Viewed: 6/8/2022 9:09:22 AM

FHEO  
Security Level: Email, Account Authentication (None)  
**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Security Level: Email, Account Authentication (None)  
**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Emily Loxha  
emily.loxha@hud.gov  
Security Level: Email, Account Authentication (None)  
**Electronic Record and Signature Disclosure:**  
Accepted: 5/19/2022 7:39:10 AM  
ID: 996524f4-4178-41aa-a464-1472fa7606ce

Witness Events	Signature	Timestamp
----------------	-----------	-----------

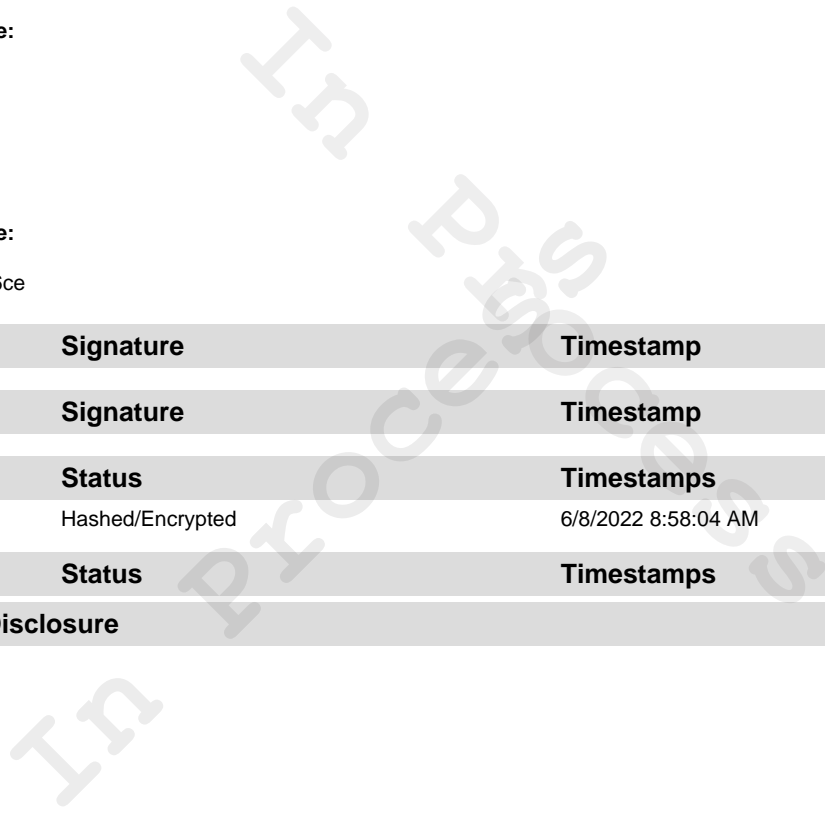
Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	6/8/2022 8:58:04 AM
---------------	------------------	---------------------

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--



## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Admin - Flexiplace (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact Admin - Flexiplace:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov)

### **To advise Admin - Flexiplace of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from Admin - Flexiplace**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with Admin - Flexiplace**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to DocuSignRequest@hud.gov and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Admin - Flexiplace as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Admin - Flexiplace during the course of your relationship with Admin - Flexiplace.

---

**From:** Frisk, Amy M  
**Sent:** Monday, June 6, 2022 12:30 PM  
**To:**  
**Cc:** Sussman, Jeffrey M  
**Subject:** Flexiplace - Remote Work Request

Dear Colleague,

At this time, your position was not approved as a remote work (100% telework) eligible position. Should the determination for your position change, you will be informed. Importantly, although the authority to make this decision was not delegated to your supervisor and was made by the Assistant Secretary or their designee, your supervisor is required to deny the request on your Flexiplace Application and Agreement Form (HUD-25228) in DocuSign to complete the process.

If you have not already done so, please feel free to submit a routine telework application to your supervisor. Please refer to [Flexiplace Information Center](#) should you have any questions.

Please note that reasonable accommodation and hardship transfer requests are not covered by this notice or the Department's Flexiplace Policy. Those requests should be submitted to the Reasonable Accommodation Branch or your supervisor under existing procedures.

*Amy M. Frisk*

Amy M. Frisk  
Acting Executive Director for Field Operations  
Office of Fair Housing and Equal Opportunity  
Department of Housing and Urban Development

---

**From:** Osegueda, Carlos  
**Sent:** Tuesday, May 24, 2022 5:11 PM  
**To:**  
**Subject:** Flexiplace Eligibility: Routine Telework

Subject: **Flexiplace Eligibility: Routine Telework**

Dear \_\_\_\_\_,

We are excited to move HUD forward under the new Flexiplace Program, which provides expanded options for workplace flexibilities. Upon completion of an initial assessment of the positions within our program office, we have determined that every position in Fair Housing and Equal Opportunity is eligible for the option of: **routine telework**. This is the maximum flexibility your position is eligible for at this time. We will continue to assess our business needs and functions of positions on an ongoing basis to determine if a different level of flexibility should be authorized in the future.

Participation in telework is voluntary. Under routine telework, you are required to report to an approved HUD office at least twice per pay period regardless of your work schedule type. The number of telework days you will be approved for is subject to supervisory approval.

If your telework application is approved for routine telework, the approval automatically includes situational telework. Under situational telework, you may request approval to use situational telework on an occasional, as needed basis. Alternatively, you may request to only participate in telework situationally and not on a regular and recurring basis.

If you are interested in teleworking, please apply via the HUD-25228 Flexiplace Application & Agreement form, routed through DocuSign, which you can access later this pay period via the [Flexiplace Information Center page on HUD@Work](#). Even if you have an existing telework agreement that you would like to keep the same, please document this arrangement by completing the form in DocuSign.

*Workspace in the HUD Office*

Please keep in mind that in the future, those employees reporting to a HUD office 6 or more days per pay period will be entitled to a dedicated office space, but those reporting to a HUD office 5 or fewer days per pay period may need to participate in a shared workspace arrangement like hoteling or hot desking. This will be implemented incrementally in most locations and after completing negotiations with our Union partners.

Please refer to the [Flexiplace Information Center](#) page for more information.

Thank you for your support.

*Jaime E. Forero*

Jaime E. Forero  
General Deputy Assistant Secretary  
Fair Housing and Equal Opportunity  
U.S Department of Housing and Urban Development



# FLEXIPLACE APPLICATION & AGREEMENT

EMPLOYEE NAME	Construction Analyst, 0828, GS13 TITLE, SERIES & GRADE
HOUSING	Housing/Multifamily/Production      mark.e.malec@hud.gov
PROGRAM OFFICE	OFFICE/DIVISION/BRANCH      IMMEDIATE SUPERVISOR E-MAIL ADDRESS
OFFICE PHONE NUMBER	400 West Bay Street, Suite 1015, Jacksonville, FL 32202 CURRENT OFFICIAL DUTY STATION ADDRESS

## TELEWORK OR REMOTE WORKSITE

ADDRESS: [REDACTED]      TELEPHONE NUMBER: [REDACTED]

CITY: [REDACTED]      COUNTY: [REDACTED]      STATE: [REDACTED]

## TYPE OF FLEXIPLACE ARRANGEMENT

**REGULAR TELEWORK - Number of days per pay period \_\_\_\_\_**

**NOTE:** If you select Regular Telework, you are automatically approved for Situational Telework.

**SITUATIONAL TELEWORK ONLY**       **COOP TELEWORK ONLY**

**NOTE:** If this application is being submitted in order to utilize only Situational or COOP telework in the future, employees must provide start and end dates and a reason/justification by email to the approving official each time telework is to be used and obtain approval in writing.

**REMOTE WORK – NEAR HUD OFFICE (within 50 miles of HUD office)**

**REMOTE WORK – OUTSIDE COMMUTING AREA (more than 50 miles from HUD office)**

## TOUR OF DUTY

**NOTE:** For employees on flexitime/flexitour schedules, start times may vary from those indicated within the applicable window.

Work Week 1	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site		Work Week 2	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site
Monday	8:30	5	TW/Remote		Monday	8:30	5	TW/Remote
Tuesday	8:30	5	TW/Remote		Tuesday	8:30	5	TW/Remote
Wednesday	8:30	5	TW/Remote		Wednesday	8:30	5	TW/Remote
Thursday	8:30	5	TW/Remote		Thursday	8:30	5	TW/Remote
Friday	8:30	5	TW/Remote		Friday	8:30	5	TW/Remote

Identify type of work to be performed at ALTERNATIVE/REMOTE worksite. Use the overflow box on the last page if more space is needed.

All work/duties OR identify specific tasks below:

EMPLOYEE AGREES TO RETRIEVE VOICE MAIL MESSAGES EVERY 4 HOURS AND TO RESPOND WITHIN 24 HOURS OR

EMPLOYEE WILL USE CALL FORWARDING FROM A HUD PHONE NUMBER OR USE A HUD-ISSUED CELL PHONE

Other Requirements: \_\_\_\_\_

## TECHNOLOGICAL INFORMATION

I have internet access at my alternative/remote worksite.     High Speed     Other (Explain): \_\_\_\_\_

I have a HUD-issued laptop.

I use a personal computer at my alternative/remote worksite in accordance with IT Helpdesk instructions because a HUD laptop is not available.

## TELEWORK/REMOTE WORKSITE SELF-CERTIFICATION SAFETY CHECKLIST

Participating employees may use the following checklist to assist them in a survey of the overall safety and adequacy of their telework/remote worksite. The following are only recommendations and do not encompass every situation that may be encountered. Employees are encouraged to obtain professional assistance with issues concerning appropriate electrical service and circuit capacity for residential worksites.

- Practice a fire evacuation plan for use in the event of an emergency.
- Check your smoke detectors regularly and replace batteries once a year.
- Always have a working fire extinguisher conveniently located in your home and check the charge regularly.
- Computers can be heavy. Always place them on sturdy, level, well maintained furniture.
- Use a sturdy chair that provides good support and can be adjusted.
- Choose office chairs that provide good supporting backrests and allow adjustments to fit you comfortably.
- Locate your computer to eliminate noticeable glare from windows and lighting. Place computer monitor at height that is comfortable and does not require neck or back strain. Locate computer keyboards at heights that do not require wrist strain or place the keyboard on an adjustable surface.
- Install sufficient lighting in locations that reduce glare at the work surface.
- Arrange file cabinets so that open drawers do not block aisles.
- Be sure to leave aisle space where possible to reduce tripping hazards.
- Always make sure electrical equipment is connected to grounded outlets.
- Avoid fire hazards by never overloading electrical circuits.
- Inspect and repair carpeting with frayed edges or loose seams. Avoid using throw rugs that can cause tripping hazards in your workspace.
- Locate computers, phones and other electrical equipment in a manner that keeps power cords out of walkways.
- Power down computers after the workday is over and always turn off all electrical equipment during thunderstorms.
- Keep your work area clean and avoid clutter, which can cause fire and tripping hazards.
- Do not allow non-government employees to operate or repair government owned equipment.
- Always keep government files and information in a secure place and do not advertise your home office to strangers.
- Always use proper lifting techniques when moving or lifting heavy equipment and furniture.
- Always report accidents and injuries immediately to your supervisor.

## RULES OF BEHAVIOR FOR REMOTE ACCESS

### ***What is the Purpose of the Remote Access Rules of Behavior?***

The intent of these HUD Remote Access Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Program Offices as a basis for their own security plans.

### ***What are Rules of Behavior?***

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish

standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

### ***Who is Covered by These Rules?***

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

### ***What is Sensitive Data?***

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

### ***What are the Penalties for Non-Compliance?***

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the HUD published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

### ***Remote Access Users:***

- Users must adhere to the HUD Standards of Conduct and behave in an ethical, informed, and trustworthy manner.
- Users will complete annual HUD Information Technology Security Awareness training. Individuals identified as having significant information privacy responsibilities must take Privacy Act training. Contact your Information System Security Officer (ISSO) for details and availability.
- Use only systems, software, and data for which you have authorization and use them only for official government business, in accordance with the most current version of the U.S. Department of Housing and Urban Development Information Technology Security Policy, Handbook 2400.25 (to be referred to as the IT Security Handbook)
- Do not attempt to override technical or management controls (i.e., sensitive data should not be downloaded to any media or removed from HUD control without prior approval, etc.).
- Take precautions to secure government information and information resources. Protect government property, including hard copy documents, from theft, destruction, or misuse.
- Properly safeguard and dispose of media (both hardcopy and electronic) using approved means of destruction in accordance with applicable records management regulations and policies. Contact your ISSO for specific instructions.
- Physically protect laptop computers from theft through the use of locking devices whenever they are not attended. Be particularly aware of the threat of loss during periods of travel.
- Utilize and store sensitive data only on HUD-approved systems or devices.
- Do not copy government information onto personally owned equipment to include personal computers, external hard drives, portable "flash drives", or media players.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect personally identifiable information to ensure that it is not disclosed to unauthorized persons, either intentionally or unintentionally and abide by the most current HUD IT Security Handbook to safeguard information.
- Use or access sensitive data outside of HUD facilities only with prior approval from your supervisor.
- Use only authorized licensed HUD software on government equipment unless authorized to do so.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up to date.
- Change passwords frequently.

- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.
- Immediately report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials. Immediately report incidents in which sensitive information has been potentially lost or compromised to the HUD HITS Help Desk. (At the time of this form's issuance, for items involving phishing, contact Phishing@hud.gov; for IT security incidents, contact CIRT@hud.gov). For example, if you lose a cell phone, laptop, removable or external hard drive, flash drive, or hardcopy documentation that contains HUD information, it should be reported without delay. Refer to the HUD IT Security Policy for additional guidance on protecting sensitive data.

**Managers:**

- Ensure that staff is given access to, and ample time to complete, the annual HUD Information Security Awareness Training.
- Should review remote access authorizations annually to ensure that a bona fide business need exists.
- Ensure that personnel granted remote access follow established HUD IT security policies, guidelines and procedures.

**Specific Privacy Act Requirements:**

- Information systems containing personally identifiable information (e.g., SSN, name, photo, and address) must be protected and may be covered by a Privacy Act System of Records (SOR) Notice. This information will have added security controls you must follow.

For more information, review the [IT Security Handbook](#)

**EMPLOYEE CERTIFICATION:** I certify all information on this application and additional forms are true and correct. I understand and agree to abide by all of the requirements of the Flexiplace Policy as well as the requirements set forth in this document and, for bargaining unit employees, in any negotiated agreements related to the Flexiplace Program. Failure to do so may result in termination from the Flexiplace Program in accordance with the HUD Flexiplace Policy and any applicable negotiated agreements. Where the policy and an applicable negotiated agreement conflict, the negotiated agreement will prevail. I understand that violation of the Rules of Behavior for Remote Access could result in punishment and/or criminal prosecution. I certify that I have read the recommendations listed in the Self Certification Safety Checklist and I understand the elements and importance of safety at my alternative worksite. Further, I understand that flexiplace arrangements are not an entitlement and this agreement may be modified or terminated at any time. I certify that I have uploaded my required training certificate or that I am an AFGE employee who completed required telework training when I previously had an approved HUD telework agreement in place.

DocuSigned by:  
 \_\_\_\_\_ 5/25/2022  
 Employee Signature Date

**APPROVING OFFICIAL:** I certify the rules set forth in the Flexiplace Policy will be enforced. Additionally, I am aware of the compensatory and overtime provisions in the Policy. Approval is contingent upon the employee meeting all technological requirements and needs. If this is a remote work request that is being approved, I have obtained this decision from the Assistant Secretary or designee.

DocuSigned by:  APPROVED  DISAPPROVED  
 \_\_\_\_\_ 5/25/2022  
 Supervisor Signature Date

Title: Branch Chief

**Reason if disapproved: Use the overflow box on the last page if more space is needed.**

Per the communication of 5/18/2022 from Mr. Jeffery Little, Associate Deputy Assistant Secretary: "Upon completion of an initial assessment of the positions within our program office, we have determined that your position is eligible for the option of: routine telework. This is the maximum flexibility your position is eligible for at this time."

### FLEXIPLACE PROGRAM COORDINATOR

I certify I have reviewed this application in its entirety and all sections are complete, properly signed and all required forms are attached.

Crystal-Diamond.C.Gibson@hud.gov

**FLEXIPLACE COORDINATOR E-MAIL ADDRESS**

**SIGNATURE:** \_\_\_\_\_ **DATE:** \_\_\_\_\_

### ATTACHMENTS

**Training Certificate:** Please upload your Telework Fundamentals training certificate here before submitting this application. If you are an AFGE bargaining unit employee and you previously had an approved HUD telework agreement in place for which you completed required training in the past, then you do not need to upload anything.

The Telework Fundamentals training currently consists of five lessons, each of which offers a lesson completion certificate. Please ensure that you upload the *final completion certificate for the entire course*, which contains no red text referring to lesson numbers. The final course completion certificate is available only after you have completed all five lessons.

**Additional Supporting Documents:** Please feel free to add additional supporting documents as needed, but do not upload any medical documents. **Supervisors:** If you add any attachments, please discuss them with your employee first.

Click the paperclip icon below to add attachments.

Employee  
click to  
attach  
certificate  
or documents

First Line  
Supervisor  
click to  
attach  
documents



**Additional space for Type of Work to be Performed at ALTERNATIVE Worksite:**

All job duties can be performed at Alternate worksite.

**Additional space for Reason for Disapproval:**

In Process

**Privacy Notice:** The information collected on this form is needed for registering and approving individuals for participation in the HUD Flexiplace Program (telework and remote work). The results from collecting this information are used to conduct audits; respond to inquiries and/or investigations as required by legal authority; and to report on aggregate data within HUD, as well as to Congress (not personally identifiable information). Personally identifiable information is protected by applicable Federal laws, including but not limited to the Privacy Act of 1974, as amended (5 U.S. Code 552a)(e)(3); the Paperwork Reduction Act of 1995; the Freedom of Information Act; and the Telework Enhancement Act of 2010, Public Law 111–292.

Print this certificate

Close this window

# *Certificate of Completion*

For:

*Telework Fundamentals - Employee Training*

Presented to:

May 20, 2022



Print this certificate

Close this window

# *Certificate of Completion*

For:

*Telework Fundamentals - Employee Training*

Presented to:

May 20, 2022





**Certificate Of Completion**

Envelope Id: EEA5344CF3034CD4AB8F4D16995AEA19	Status: Sent
Subject: Flexiplace Application for	
Source Envelope:	
Document Pages: 8	Signatures: 2
Certificate Pages: 5	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Return to Work Questions
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	451 7th Street NW
	Washington, DC 20410
	ReturntoWorkQuestions@hud.gov
	IP Address: 170.97.91.25

**Record Tracking**

Status: Original	Holder: Return to Work Questions	Location: DocuSign
5/25/2022 7:23:21 AM	ReturntoWorkQuestions@hud.gov	
Security Appliance Status: Connected	Pool: FedRamp	
Storage Appliance Status: Connected	Pool: Admin - Flexiplace	Location: DocuSign

**Signer Events**

**Signature**

**Timestamp**

DocuSign.email  
ID: 1  
5/25/2022 7:23:25 AM

Signature Adoption: Pre-selected Style  
Signed by link sent to

Using IP Address: 170.97.91.25

Sent: 5/25/2022 7:23:24 AM  
Viewed: 5/25/2022 7:23:53 AM  
Signed: 5/25/2022 7:40:56 AM

**Electronic Record and Signature Disclosure:**  
Accepted: 5/25/2022 7:23:53 AM  
ID: e6d6b1a8-fca0-4c91-a9d4-92e34109a3af

Mark Malec  
mark.e.malec@hud.gov  
Security Level: Email, Account Authentication (None)

DocuSigned by:  
*Mark Malec*  
2FEA40F98E0040E...

Signature Adoption: Pre-selected Style  
Signed by link sent to mark.e.malec@hud.gov  
Using IP Address: 170.97.91.25

Sent: 5/25/2022 7:41:01 AM  
Viewed: 5/25/2022 7:59:42 AM  
Signed: 5/25/2022 11:32:38 AM

**Electronic Record and Signature Disclosure:**  
Accepted: 5/25/2022 11:31:58 AM  
ID: 0694db33-6dd2-4711-9a1b-162ce3fe83ce

Crystal-Diamond C. Gibson  
Crystal-Diamond.C.Gibson@hud.gov  
Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Sent: 5/25/2022 11:32:42 AM

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

**COPIED**

Sent: 5/25/2022 7:41:00 AM  
Viewed: 5/25/2022 7:52:54 AM

Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Mark Malec  
mark.e.malec@hud.gov

Security Level: Email, Account Authentication (None)

**Electronic Record and Signature Disclosure:**  
Accepted: 5/25/2022 11:31:58 AM  
ID: 0694db33-6dd2-4711-9a1b-162ce3fe83ce

Witness Events	Signature	Timestamp
----------------	-----------	-----------

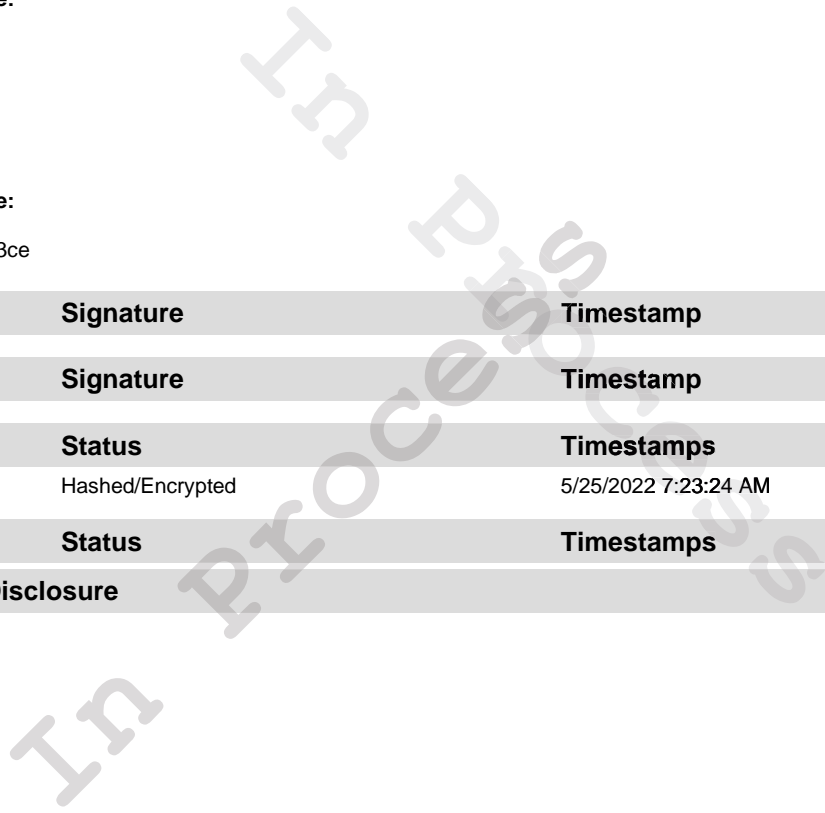
Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	5/25/2022 7:23:24 AM
---------------	------------------	----------------------

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--



## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, Admin - Flexiplace (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact Admin - Flexiplace:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov)

### **To advise Admin - Flexiplace of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from Admin - Flexiplace**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [DocuSignRequest@hud.gov](mailto:DocuSignRequest@hud.gov) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with Admin - Flexiplace**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to DocuSignRequest@hud.gov and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Admin - Flexiplace as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Admin - Flexiplace during the course of your relationship with Admin - Flexiplace.

# FLEXIPLACE APPLICATION & AGREEMENT

EMPLOYEE NAME	Environmental Protection Special GS-13
CPD	TITLE, SERIES & GRADE
PROGRAM OFFICE	Martha.A.Curran@hud.gov
OFFICE/DIVISION/BRANCH	IMMEDIATE SUPERVISOR E-MAIL ADDRESS
OFFICE PHONE NUMBER	1500 Pinecroft Road, Suite 401, Greensboro, NC 27407
CURRENT OFFICIAL DUTY STATION ADDRESS	

## TELEWORK OR REMOTE WORKSITE

ADDRESS: [REDACTED] TELEPHONE NUMBER [REDACTED]

CITY: [REDACTED] COUNTY: [REDACTED] STATE: [REDACTED]

## TYPE OF FLEXIPLACE ARRANGEMENT

**REGULAR TELEWORK - Number of days per pay period \_\_\_\_\_**

**NOTE:** If you select Regular Telework, you are automatically approved for Situational Telework.

**SITUATIONAL TELEWORK ONLY**       **COOP TELEWORK ONLY**

**NOTE:** If this application is being submitted in order to utilize only Situational or COOP telework in the future, employees must provide start and end dates and a reason/justification by email to the approving official each time telework is to be used and obtain approval in writing.

**REMOTE WORK – NEAR HUD OFFICE (within 50 miles of HUD office)**

**REMOTE WORK – OUTSIDE COMMUTING AREA (more than 50 miles from HUD office)**

## TOUR OF DUTY

**NOTE:** For employees on flexitime/flexitour schedules, start times may vary from those indicated within the applicable window.

Work Week 1	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site		Work Week 2	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site
Monday	8:00 am	4:30 pm	TW/Remote		Monday	8:00 am	4:30 pm	TW/Remote
Tuesday	8:00 am	4:30 pm	TW/Remote		Tuesday	8:00 am	4:30 pm	TW/Remote
Wednesday	8:00 am	4:30 pm	TW/Remote		Wednesday	8:00 am	4:30 pm	TW/Remote
Thursday	8:00 am	4:30 pm	TW/Remote		Thursday	8:00 am	4:30 pm	TW/Remote
Friday	8:00 am	4:30 pm	TW/Remote		Friday	8:00 am	4:30 pm	TW/Remote

Identify type of work to be performed at ALTERNATIVE/REMOTE worksite. Use the overflow box on the last page if more space is needed.

All work/duties OR identify specific tasks below:

EMPLOYEE AGREES TO RETRIEVE VOICE MAIL MESSAGES EVERY 2 HOURS AND TO RESPOND WITHIN 2 HOURS OR

EMPLOYEE WILL USE CALL FORWARDING FROM A HUD PHONE NUMBER OR USE A HUD-ISSUED CELL PHONE

Other Requirements: \_\_\_\_\_

## TECHNOLOGICAL INFORMATION

I have internet access at my alternative/remote worksite.     High Speed     Other (Explain): \_\_\_\_\_

I have a HUD-issued laptop.

I use a personal computer at my alternative/remote worksite in accordance with IT Helpdesk instructions because a HUD laptop is not available.

## TELEWORK/REMOTE WORKSITE SELF-CERTIFICATION SAFETY CHECKLIST

Participating employees may use the following checklist to assist them in a survey of the overall safety and adequacy of their telework/remote worksite. The following are only recommendations and do not encompass every situation that may be encountered. Employees are encouraged to obtain professional assistance with issues concerning appropriate electrical service and circuit capacity for residential worksites.

- Practice a fire evacuation plan for use in the event of an emergency.
- Check your smoke detectors regularly and replace batteries once a year.
- Always have a working fire extinguisher conveniently located in your home and check the charge regularly.
- Computers can be heavy. Always place them on sturdy, level, well maintained furniture.
- Use a sturdy chair that provides good support and can be adjusted.
- Choose office chairs that provide good supporting backrests and allow adjustments to fit you comfortably.
- Locate your computer to eliminate noticeable glare from windows and lighting. Place computer monitor at height that is comfortable and does not require neck or back strain. Locate computer keyboards at heights that do not require wrist strain or place the keyboard on an adjustable surface.
- Install sufficient lighting in locations that reduce glare at the work surface.
- Arrange file cabinets so that open drawers do not block aisles.
- Be sure to leave aisle space where possible to reduce tripping hazards.
- Always make sure electrical equipment is connected to grounded outlets.
- Avoid fire hazards by never overloading electrical circuits.
- Inspect and repair carpeting with frayed edges or loose seams. Avoid using throw rugs that can cause tripping hazards in your workspace.
- Locate computers, phones and other electrical equipment in a manner that keeps power cords out of walkways.
- Power down computers after the workday is over and always turn off all electrical equipment during thunderstorms.
- Keep your work area clean and avoid clutter, which can cause fire and tripping hazards.
- Do not allow non-government employees to operate or repair government owned equipment.
- Always keep government files and information in a secure place and do not advertise your home office to strangers.
- Always use proper lifting techniques when moving or lifting heavy equipment and furniture.
- Always report accidents and injuries immediately to your supervisor.

## RULES OF BEHAVIOR FOR REMOTE ACCESS

### ***What is the Purpose of the Remote Access Rules of Behavior?***

The intent of these HUD Remote Access Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Program Offices as a basis for their own security plans.

### ***What are Rules of Behavior?***

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish

standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

### ***Who is Covered by These Rules?***

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

### ***What is Sensitive Data?***

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

### ***What are the Penalties for Non-Compliance?***

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the HUD published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

### ***Remote Access Users:***

- Users must adhere to the HUD Standards of Conduct and behave in an ethical, informed, and trustworthy manner.
- Users will complete annual HUD Information Technology Security Awareness training. Individuals identified as having significant information privacy responsibilities must take Privacy Act training. Contact your Information System Security Officer (ISSO) for details and availability.
- Use only systems, software, and data for which you have authorization and use them only for official government business, in accordance with the most current version of the U.S. Department of Housing and Urban Development Information Technology Security Policy, Handbook 2400.25 (to be referred to as the IT Security Handbook)
- Do not attempt to override technical or management controls (i.e., sensitive data should not be downloaded to any media or removed from HUD control without prior approval, etc.).
- Take precautions to secure government information and information resources. Protect government property, including hard copy documents, from theft, destruction, or misuse.
- Properly safeguard and dispose of media (both hardcopy and electronic) using approved means of destruction in accordance with applicable records management regulations and policies. Contact your ISSO for specific instructions.
- Physically protect laptop computers from theft through the use of locking devices whenever they are not attended. Be particularly aware of the threat of loss during periods of travel.
- Utilize and store sensitive data only on HUD-approved systems or devices.
- Do not copy government information onto personally owned equipment to include personal computers, external hard drives, portable "flash drives", or media players.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect personally identifiable information to ensure that it is not disclosed to unauthorized persons, either intentionally or unintentionally and abide by the most current HUD IT Security Handbook to safeguard information.
- Use or access sensitive data outside of HUD facilities only with prior approval from your supervisor.
- Use only authorized licensed HUD software on government equipment unless authorized to do so.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up to date.
- Change passwords frequently.



- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.
- Immediately report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials. Immediately report incidents in which sensitive information has been potentially lost or compromised to the HUD HITS Help Desk. (At the time of this form's issuance, for items involving phishing, contact Phishing@hud.gov; for IT security incidents, contact CIRT@hud.gov). For example, if you lose a cell phone, laptop, removable or external hard drive, flash drive, or hardcopy documentation that contains HUD information, it should be reported without delay. Refer to the HUD IT Security Policy for additional guidance on protecting sensitive data.

**Managers:**

- Ensure that staff is given access to, and ample time to complete, the annual HUD Information Security Awareness Training.
- Should review remote access authorizations annually to ensure that a bona fide business need exists.
- Ensure that personnel granted remote access follow established HUD IT security policies, guidelines and procedures.

**Specific Privacy Act Requirements:**

- Information systems containing personally identifiable information (e.g., SSN, name, photo, and address) must be protected and may be covered by a Privacy Act System of Records (SOR) Notice. This information will have added security controls you must follow.

For more information, review the [IT Security Handbook](#)

**EMPLOYEE CERTIFICATION:** I certify all information on this application and additional forms are true and correct. I understand and agree to abide by all of the requirements of the Flexiplace Policy as well as the requirements set forth in this document and, for bargaining unit employees, in any negotiated agreements related to the Flexiplace Program. Failure to do so may result in termination from the Flexiplace Program in accordance with the HUD Flexiplace Policy and any applicable negotiated agreements. Where the policy and an applicable negotiated agreement conflict, the negotiated agreement will prevail. I understand that violation of the Rules of Behavior for Remote Access could result in punishment and/or criminal prosecution. I certify that I have read the recommendations listed in the Self Certification Safety Checklist and I understand the elements and importance of safety at my alternative worksite. Further, I understand that flexiplace arrangements are not an entitlement and this agreement may be modified or terminated at any time. I certify that I have uploaded my required training certificate or that I am an AFGE employee who completed required telework training when I previously had an approved HUD telework agreement in place.

DocuSigned by: \_\_\_\_\_ 5/27/2022

Employee Signature \_\_\_\_\_ Date

**APPROVING OFFICIAL:** I certify the rules set forth in the Flexiplace Policy will be enforced. Additionally, I am aware of the compensatory and overtime provisions in the Policy. Approval is contingent upon the employee meeting all technological requirements and needs. If this is a remote work request that is being approved, I have obtained this decision from the Assistant Secretary or designee.

DocuSigned by:  APPROVED  DISAPPROVED

*Martha A. Curran* \_\_\_\_\_ 6/1/2022

Supervisor Signature \_\_\_\_\_ Date

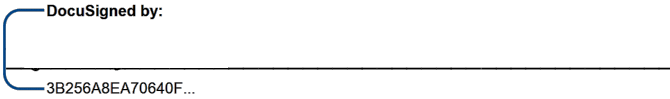
Title: Regional Environmental Officer

**Reason if disapproved:** Use the overflow box on the last page if more space is needed.  
Your position was not approved as a remote work eligible position at this time. Should the determination for your position change, you will be informed.

### FLEXIPLACE PROGRAM COORDINATOR

I certify I have reviewed this application in its entirety and all sections are complete, properly signed and all required forms are attached.

\_\_\_\_\_  
**FLEXIPLACE COORDINATOR E-MAIL ADDRESS**

**SIGNATURE:**  **DATE:** 6/1/2022

### ATTACHMENTS

**Training Certificate:** Please upload your Telework Fundamentals training certificate here before submitting this application. If you are an AFGE bargaining unit employee and you previously had an approved HUD telework agreement in place for which you completed required training in the past, then you do not need to upload anything.

The Telework Fundamentals training currently consists of five lessons, each of which offers a lesson completion certificate. Please ensure that you upload the *final completion certificate for the entire course*, which contains no red text referring to lesson numbers. The final course completion certificate is available only after you have completed all five lessons.

**Additional Supporting Documents:** Please feel free to add additional supporting documents as needed, but do not upload any medical documents. **Supervisors:** If you add any attachments, please discuss them with your employee first.

Click the paperclip icon below to add attachments.

Employee  
click to  
attach  
certificate  
or documents

First Line  
Supervisor  
click to  
attach  
documents



**Additional space for Type of Work to be Performed at ALTERNATIVE Worksite:**

**Additional space for Reason for Disapproval:**

**Privacy Notice:** The information collected on this form is needed for registering and approving individuals for participation in the HUD Flexiplace Program (telework and remote work). The results from collecting this information are used to conduct audits; respond to inquiries and/or investigations as required by legal authority; and to report on aggregate data within HUD, as well as to Congress (not personally identifiable information). Personally identifiable information is protected by applicable Federal laws, including but not limited to the Privacy Act of 1974, as amended (5 U.S. Code 552a)(e)(3); the Paperwork Reduction Act of 1995; the Freedom of Information Act; and the Telework Enhancement Act of 2010, Public Law 111–292.

# FLEXIPLACE APPLICATION & AGREEMENT

<b>EMPLOYEE NAME</b>	Contract Specialist, 1102, 13
	<b>TITLE, SERIES &amp; GRADE</b>
OCPO	OCPO
	Sharon.L.washington@hud.gov
<b>PROGRAM OFFICE</b>	<b>OFFICE/DIVISION/BRANCH</b>
	<b>IMMEDIATE SUPERVISOR E-MAIL ADDRESS</b>
	Telework address
<b>OFFICE PHONE NUMBER</b>	<b>CURRENT OFFICIAL DUTY STATION ADDRESS</b>

## TELEWORK OR REMOTE WORKSITE

**ADDRESS:** [REDACTED] **TELEPHONE NUMBER:** [REDACTED]

**CITY:** [REDACTED] **COUNTY:** [REDACTED] **STATE:** [REDACTED]

## TYPE OF FLEXIPLACE ARRANGEMENT

**REGULAR TELEWORK - Number of days per pay period \_\_\_\_\_**

**NOTE:** If you select Regular Telework, you are automatically approved for Situational Telework.

**SITUATIONAL TELEWORK ONLY**       **COOP TELEWORK ONLY**

**NOTE:** If this application is being submitted in order to utilize only Situational or COOP telework in the future, employees must provide start and end dates and a reason/justification by email to the approving official each time telework is to be used and obtain approval in writing.

**REMOTE WORK – NEAR HUD OFFICE (within 50 miles of HUD office)**

**REMOTE WORK – OUTSIDE COMMUTING AREA (more than 50 miles from HUD office)**

## TOUR OF DUTY

**NOTE:** For employees on flexitime/flexitour schedules, start times may vary from those indicated within the applicable window.

Work Week 1	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site		Work Week 2	Start Time	End Time	LOCATION: HUD Office or Telework/Remote Site
Monday	7:30am	4:00pm	TW/Remote		Monday	7:30am	4:00pm	TW/Remote
Tuesday	7:30am	4:00pm	TW/Remote		Tuesday	7:30am	4:00pm	TW/Remote
Wednesday	7:30am	4:00pm	TW/Remote		Wednesday	7:30am	4:00pm	TW/Remote
Thursday	7:30am	4:00pm	TW/Remote		Thursday	7:30am	4:00pm	TW/Remote
Friday	7:30am	4:00pm	TW/Remote		Friday	7:30am	4:00pm	TW/Remote

Identify type of work to be performed at ALTERNATIVE/REMOTE worksite. Use the overflow box on the last page if more space is needed.

**All work/duties OR identify specific tasks below:**

**EMPLOYEE AGREES TO RETRIEVE VOICE MAIL MESSAGES EVERY 2 HOURS AND TO RESPOND WITHIN 2 HOURS OR**

**EMPLOYEE WILL USE CALL FORWARDING FROM A HUD PHONE NUMBER OR USE A HUD-ISSUED CELL PHONE**

Other Requirements: \_\_\_\_\_

## TECHNOLOGICAL INFORMATION

**I have internet access at my alternative/remote worksite.**     **High Speed**     **Other (Explain):** \_\_\_\_\_

**I have a HUD-issued laptop.**

**I use a personal computer at my alternative/remote worksite in accordance with IT Helpdesk instructions because a HUD laptop is not available.**

## TELEWORK/REMOTE WORKSITE SELF-CERTIFICATION SAFETY CHECKLIST

Participating employees may use the following checklist to assist them in a survey of the overall safety and adequacy of their telework/remote worksite. The following are only recommendations and do not encompass every situation that may be encountered. Employees are encouraged to obtain professional assistance with issues concerning appropriate electrical service and circuit capacity for residential worksites.

- Practice a fire evacuation plan for use in the event of an emergency.
- Check your smoke detectors regularly and replace batteries once a year.
- Always have a working fire extinguisher conveniently located in your home and check the charge regularly.
- Computers can be heavy. Always place them on sturdy, level, well maintained furniture.
- Use a sturdy chair that provides good support and can be adjusted.
- Choose office chairs that provide good supporting backrests and allow adjustments to fit you comfortably.
- Locate your computer to eliminate noticeable glare from windows and lighting. Place computer monitor at height that is comfortable and does not require neck or back strain. Locate computer keyboards at heights that do not require wrist strain or place the keyboard on an adjustable surface.
- Install sufficient lighting in locations that reduce glare at the work surface.
- Arrange file cabinets so that open drawers do not block aisles.
- Be sure to leave aisle space where possible to reduce tripping hazards.
- Always make sure electrical equipment is connected to grounded outlets.
- Avoid fire hazards by never overloading electrical circuits.
- Inspect and repair carpeting with frayed edges or loose seams. Avoid using throw rugs that can cause tripping hazards in your workspace.
- Locate computers, phones and other electrical equipment in a manner that keeps power cords out of walkways.
- Power down computers after the workday is over and always turn off all electrical equipment during thunderstorms.
- Keep your work area clean and avoid clutter, which can cause fire and tripping hazards.
- Do not allow non-government employees to operate or repair government owned equipment.
- Always keep government files and information in a secure place and do not advertise your home office to strangers.
- Always use proper lifting techniques when moving or lifting heavy equipment and furniture.
- Always report accidents and injuries immediately to your supervisor.

## RULES OF BEHAVIOR FOR REMOTE ACCESS

### ***What is the Purpose of the Remote Access Rules of Behavior?***

The intent of these HUD Remote Access Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Program Offices as a basis for their own security plans.

### ***What are Rules of Behavior?***

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish

standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

### ***Who is Covered by These Rules?***

These rules extend to all HUD personnel and any other persons using HUD IT equipment or accessing HUD systems under formally established agreements. This includes contractors and other federally funded users. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

### ***What is Sensitive Data?***

Sensitive data is data that must be protected on the basis of its need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

### ***What are the Penalties for Non-Compliance?***

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. HUD will enforce the use of penalties against any user who willfully violates any HUD or federal system security (and related) policy as appropriate.

These Rules of Behavior are founded on the principles described in the HUD published security policy and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

### ***Remote Access Users:***

- Users must adhere to the HUD Standards of Conduct and behave in an ethical, informed, and trustworthy manner.
- Users will complete annual HUD Information Technology Security Awareness training. Individuals identified as having significant information privacy responsibilities must take Privacy Act training. Contact your Information System Security Officer (ISSO) for details and availability.
- Use only systems, software, and data for which you have authorization and use them only for official government business, in accordance with the most current version of the U.S. Department of Housing and Urban Development Information Technology Security Policy, Handbook 2400.25 (to be referred to as the IT Security Handbook)
- Do not attempt to override technical or management controls (i.e., sensitive data should not be downloaded to any media or removed from HUD control without prior approval, etc.).
- Take precautions to secure government information and information resources. Protect government property, including hard copy documents, from theft, destruction, or misuse.
- Properly safeguard and dispose of media (both hardcopy and electronic) using approved means of destruction in accordance with applicable records management regulations and policies. Contact your ISSO for specific instructions.
- Physically protect laptop computers from theft through the use of locking devices whenever they are not attended. Be particularly aware of the threat of loss during periods of travel.
- Utilize and store sensitive data only on HUD-approved systems or devices.
- Do not copy government information onto personally owned equipment to include personal computers, external hard drives, portable "flash drives", or media players.
- Do not alter the configuration, including installing software or peripherals, on government equipment unless authorized.
- Protect personally identifiable information to ensure that it is not disclosed to unauthorized persons, either intentionally or unintentionally and abide by the most current HUD IT Security Handbook to safeguard information.
- Use or access sensitive data outside of HUD facilities only with prior approval from your supervisor.
- Use only authorized licensed HUD software on government equipment unless authorized to do so.
- Adhere to all provisions or agreements related to off-site work.
- Use virus protection software on off-site systems and keep it up to date.
- Change passwords frequently.

- Protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the computer.
- Immediately report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials. Immediately report incidents in which sensitive information has been potentially lost or compromised to the HUD HITS Help Desk. (At the time of this form's issuance, for items involving phishing, contact Phishing@hud.gov; for IT security incidents, contact CIRT@hud.gov). For example, if you lose a cell phone, laptop, removable or external hard drive, flash drive, or hardcopy documentation that contains HUD information, it should be reported without delay. Refer to the HUD IT Security Policy for additional guidance on protecting sensitive data.

**Managers:**

- Ensure that staff is given access to, and ample time to complete, the annual HUD Information Security Awareness Training.
- Should review remote access authorizations annually to ensure that a bona fide business need exists.
- Ensure that personnel granted remote access follow established HUD IT security policies, guidelines and procedures.

**Specific Privacy Act Requirements:**

- Information systems containing personally identifiable information (e.g., SSN, name, photo, and address) must be protected and may be covered by a Privacy Act System of Records (SOR) Notice. This information will have added security controls you must follow.

For more information, review the [IT Security Handbook](#)

**EMPLOYEE CERTIFICATION:** I certify all information on this application and additional forms are true and correct. I understand and agree to abide by all of the requirements of the Flexiplace Policy as well as the requirements set forth in this document and, for bargaining unit employees, in any negotiated agreements related to the Flexiplace Program. Failure to do so may result in termination from the Flexiplace Program in accordance with the HUD Flexiplace Policy and any applicable negotiated agreements. Where the policy and an applicable negotiated agreement conflict, the negotiated agreement will prevail. I understand that violation of the Rules of Behavior for Remote Access could result in punishment and/or criminal prosecution. I certify that I have read the recommendations listed in the Self Certification Safety Checklist and I understand the elements and importance of safety at my alternative worksite. Further, I understand that flexiplace arrangements are not an entitlement and this agreement may be modified or terminated at any time. I certify that I have uploaded my required training certificate or that I am an AFGE employee who completed required telework training when I previously had an approved HUD telework agreement in place.

DocuSigned by:  
 \_\_\_\_\_ 6/2/2022  
 Employee Signature Date

**APPROVING OFFICIAL:** I certify the rules set forth in the Flexiplace Policy will be enforced. Additionally, I am aware of the compensatory and overtime provisions in the Policy. Approval is contingent upon the employee meeting all technological requirements and needs. If this is a remote work request that is being approved, I have obtained this decision from the Assistant Secretary or designee.

DocuSigned by:  
 APPROVED  DISAPPROVED  
 \_\_\_\_\_ 6/2/2022  
 Supervisor Signature Date

Title: Division Director

**Reason if disapproved: Use the overflow box on the last page if more space is needed.**

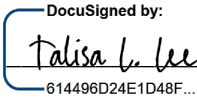
Your position is not eligible for remote telework. If this changes in the future you will be informed.

### FLEXIPLACE PROGRAM COORDINATOR

I certify I have reviewed this application in its entirety and all sections are complete, properly signed and all required forms are attached.

talisa.l.lee@hud.gov

#### FLEXIPLACE COORDINATOR E-MAIL ADDRESS

**SIGNATURE:**  **DATE:** 6/3/2022

### ATTACHMENTS

**Training Certificate:** Please upload your Telework Fundamentals training certificate here before submitting this application. If you are an AFGE bargaining unit employee and you previously had an approved HUD telework agreement in place for which you completed required training in the past, then you do not need to upload anything.

The Telework Fundamentals training currently consists of five lessons, each of which offers a lesson completion certificate. Please ensure that you upload the *final completion certificate for the entire course*, which contains no red text referring to lesson numbers. The final course completion certificate is available only after you have completed all five lessons.

**Additional Supporting Documents:** Please feel free to add additional supporting documents as needed, but do not upload any medical documents. **Supervisors:** If you add any attachments, please discuss them with your employee first.

Click the paperclip icon below to add attachments.

Employee  
click to  
attach  
certificate  
or documents

First Line  
Supervisor  
click to  
attach  
documents





**Additional space for Type of Work to be Performed at ALTERNATIVE Worksite:**

**Additional space for Reason for Disapproval:**

**Privacy Notice:** The information collected on this form is needed for registering and approving individuals for participation in the HUD Flexiplace Program (telework and remote work). The results from collecting this information are used to conduct audits; respond to inquiries and/or investigations as required by legal authority; and to report on aggregate data within HUD, as well as to Congress (not personally identifiable information). Personally identifiable information is protected by applicable Federal laws, including but not limited to the Privacy Act of 1974, as amended (5 U.S. Code 552a)(e)(3); the Paperwork Reduction Act of 1995; the Freedom of Information Act; and the Telework Enhancement Act of 2010, Public Law 111–292.