



RULES OF BEHAVIOR

Office of Information Management and Technology (OMT)

U.S. Department of Housing and Urban Development

Office of Inspector General

451 7th Street, SW

Suite 8254

Washington, DC 20410

April 2016

Document History

The Rules of Behavior shall be updated every twelve (12) months or whenever there are significant changes to the information system, the facilities where the systems reside, or other conditions that may impact the security or accreditation status of the system.

Release No.	Date	Sections Revised	Revision Description
1.0	2007	All	Initial Release
2.0	2008	All	Rewrite
2.4	2009	All	Update various sections to require the use of VPN for any external access. Section 4.2 added the requirement not to post to social networking sites. Expanded the acknowledgement statement.
2.5	2009	All	Final grammatical edit
3.0	April 2009	All	Final approved annual update
4.0	March 2010	Section 4.4	Update to Wireless connectivity
5.0	August 2012	Section 4.3 and 4.4	Update to MS Outlook Web Access (OWA and Citrix Access Gateway (CAG).
6.0	May 2014	Whole document	Reviewed the whole document and removed outdated instructions. Added MyPC.hudoig.gov portal.
7.0	Dec 2014	Whole document	Reviewed the whole document and updated technology references.
8.0	April 2016	Whole document	Reviewed the whole document and updated technology references.

Contents

Document History 2

Contents 3

1. General 4

 1.1 Purpose 4

 1.2 Scope 4

2. Email Use 5

3. User Identification (User ID) and Password Usage 5

4. Access 6

 4.1 System Access 6

 4.2 Internet Access 6

 4.3 Remote Access 7

 4.4 Wireless Access 7

5. Hardware and Software 8

6. Teleworking 8

7. Video Teleconference and Instant Messaging (IM) capabilities 9

8. Personally Identifiable Information (PII) 9

9. Disciplinary Actions 10

10. Acknowledgment Statement 11

1. General

1.1 Purpose

The purpose of this document is to provide governance for the acceptable use of HUD OIG information technology (IT) systems and resources by HUD OIG employees, contractors, vendors, and others. HUD OIG resources and data are the property of the Federal Government and must be protected. Any user who is found to have violated any HUD OIG policy may be subject to disciplinary action as stated in OIGM 1752, *Disciplinary and Adverse Actions*.

Your access to computing resources indicates a level of trust given to you by HUD OIG management. The Rules of Behavior presented in this document highlight requirements from several laws, policies, and best practices. The Rules of Behavior establish acceptable computing behaviors. Because written guidance cannot cover every contingency, users are also expected to use sound judgment and the highest ethical standards in their decision-making. Users must be aware of and acknowledge their actions and responsibilities when using HUD OIG resources in accordance with the Rules of Behavior.

1.2 Scope

The Rules of Behavior do not replace existing HUD OIG security policies or directives. Rather, they supplement and further articulate existing security policies and practices and are consistent with the following HUD OIG manual chapters:

- OIGM CHAPTER 1031, [Records Managements](#)
- OIGM CHAPTER 1054, [OIG Office Automation](#)
- OIGM CHAPTER 1054.1, [Information Technology Security Policy](#)
- OIGM CHAPTER 1054.2, [Breach Notification Response Plan](#)
- OIGM CHAPTER 1054.3, [Internet Use and Web Monitoring Policy](#)
- OIGM CHAPTER 1054.4, [OIG E-mail Management Procedures](#)
- OIGM CHAPTER 1054.5, [OIG System Access User Guide](#)
- OIGM CHAPTER 1083, [Standards of Conduct and Other Requirements](#)
- OIGM CHAPTER 1120, [Personal Property Management](#)
- OIGM CHAPTER 1611, [Telework Program](#)
- OIGM CHAPTER 1731, [Personnel Security and Suitability](#)
- OIGM CHAPTER 1752, [Disciplinary and Adverse Actions](#)

2. Email Use

HUD OIG uses email correspondence to perform government business. Users are entrusted to use this resource to perform their duties. As an authorized HUD OIG user, these are your responsibilities in regards to the use of HUD OIG email accounts:

1. Limit use of the HUD OIG email system for personal purposes to non-work time, with the understanding that use of the HUD OIG email system is to conduct official business and it is considered a formal government public record to which there is no expectation of privacy or confidentiality.
2. Do not use personal email accounts to conduct government business.
3. Do not open suspicious or unfamiliar emails or email attachments.
4. Report virus or other malware warnings immediately to the HUD OIG Help Desk¹.
5. Do not forward HUD OIG business emails to personal accounts.
6. Do not intentionally or negligently cause the propagation of malware (viruses, trojan horses, or other malicious software).
7. Do not use the HUD OIG email system for the creation or distribution of any disruptive or offensive messages.

3. User Identification (User ID) and Password Usage

Authentication is the process of verifying the identity of a user, usually as a prerequisite for granting access to resources in an IT system. As an authorized HUD OIG user, these are your responsibilities regarding the use of HUD OIG user accounts and passwords:

1. Immediately report to the HUD OIG Help Desk to have your password or Smart Card PIN changed should it become compromised.
2. Memorize your passwords.
3. Do not write your passwords on paper or store them anywhere, physically or electronically without strong encryption.
4. Create unique passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters.
5. Do not choose passwords based upon details that may not be as confidential as you'd expect, such as your birth date, your Social Security or phone number, or names of family members.
6. Do not share your username(s)/password(s) with anyone.
7. Do not use your personal or social media passwords as any of your HUD OIG system passwords.
8. Do not ask anyone for their username(s)/password(s).
9. Report immediately to the HUD OIG Help Desk any misuse of username(s)/password(s).

¹ Contact the IT Customer Service Center at ITCustomerServiceCenter@hudoig.gov or 1-866-614-6676.

4. Access

4.1 System Access

Access is the ability to use any HUD OIG resource for which you have official authorization. As an authorized HUD OIG user, these are your responsibilities regarding the access to HUD OIG systems:

1. Abide by the established guidelines for usernames/passwords, user authentication, and physical security procedures.
2. Refrain from bypassing any encryption method, authentication method, or physical security measure in any way.
3. Report all unauthorized access to HUD OIG data and IT resources to the HUD OIG Help Desk² during duty hours or to the HUD OIG Duty Officer during non-duty hours. (The contact information for both entities is provided below.)
4. Do not provide any type of information to individuals outside of the organization, individuals who do not have a need to know, or individuals without the authority to access HUD OIG data or IT resources.
5. Do not allow non HUD OIG individuals to access HUD OIG resources or systems.

HUD OIG Help Desk: **Phone:** (1-866) 614-6676 **Email:** helpdesk@hudoig.gov

HUD OIG Duty Officer: **Phone:** (202) 708-5998

4.2 Internet Access

Users must act in accordance with OIGM 1054.3, *Internet Use and Web Monitoring Policy*, when accessing the internet on the HUD OIG network. As an authorized HUD OIG user, these are your responsibilities for internet access on the HUD OIG network:

1. Access the Internet only through an approved HUD OIG connection at a HUD OIG facility or off-site through the HUD OIG virtual private network (VPN).
2. Limit personal Internet browsing when connected to the HUD OIG network, remembering that all internet activity is logged and that there is no right to privacy or confidentiality.
3. Do not visit websites that promote, display, discuss, share, or distribute hateful, racist, obscene, pornographic, or illegal activity or any similar type of behavior.
4. Be cautious of social engineering when you post to social networking sites such as Facebook, LinkedIn, Twitter or any other social media sites.
5. Do not access HUD OIG resources to manage, run, supervise, or conduct personal business enterprises.
6. Do not use HUD OIG resources for harassment of any kind.

² Contact the IT Customer Service Center at ITCustomerServiceCenter@hudoig.gov or 1-866-614-6676.

HUD OIG OMT Rules of Behavior

7. Do not use HUD OIG resources for anything that limits productivity or causes service interruptions. Streaming audio and video (i.e. music and TV/movies) are particularly heavy consumers of network bandwidth and should not be used on the HUD OIG network unless for valid business purposes.
8. Do not access HUD OIG resources to engage in prohibited political activities in compliance with the Hatch Act.

4.3 Remote Access

Remote access is the access to HUD OIG resources from a location not under the direct control of HUD OIG; this includes “telework” environments as well as off-site audit/investigation locations. As an authorized HUD OIG user, these are your responsibilities regarding remote access to the HUD OIG network:

1. Access HUD OIG resources only through the HUD OIG VPN connection or MyPC.hudoig.gov portal.
2. Connect HUD OIG-issued devices only through the approved HUD OIG VPN.
3. Use only HUD OIG-issued laptops, workstations, and mobile devices to access HUD OIG resources; the only exceptions are Microsoft Outlook Web Access (OWA) and MyPC.hudoig.gov.
4. Do not print sensitive HUD OIG documents or other data on personally owned home printers or on non-HUD OIG devices, such as those at hotels.
5. Secure all mobile/portable HUD OIG resources (e.g., laptops, mobile devices, thumb drives, etc.) when not in use and outside of HUD OIG facilities.
6. It is the responsibility of HUD OIG staff to make sure personal computers used to access HUD OIG resources and systems remotely are fully patched and secured with an antimalware solution.
7. Do not allow non HUD OIG individuals to access internet from HUD OIG resources. HUD OIG personnel bear responsibility for the consequences should access be misused.
8. Ensure that home/personal internet routers/modems including, cable, fiber, DSL or other types of internet access devices used to access the HUD OIG network, are at least configured to require password using WPA2 Personal wireless security. Contact your Internet Service Provider for assistance.
9. Do not reconfigure HUD OIG equipment at any time.
10. Secure HUD OIG information (hard copy and electronic media) when not in use and outside of HUD OIG controlled facilities.

4.4 Wireless Access

As an authorized HUD OIG user, these are your responsibilities regarding wireless access to the HUD OIG network:

1. Connect only authorized wireless devices to HUD OIG resources (e.g., issued wireless devices from the [Approved Hardware List](#))³.

³ The Approved Hardware List can be found here: <http://collaboration/sites/ask-it/documents/currentapprovedhardwarelist.pdf>

HUD OIG OMT Rules of Behavior

2. Use only the HUD OIG-approved VPN client when connecting through any public wireless access point or wireless device (e.g., airports, hotels, etc.) to access HUD OIG resources, except if using MyPC.hudoig.gov or Microsoft Outlook Web Access (OWA).

5. Hardware and Software

As an authorized HUD OIG user, these are your responsibilities regarding the use of HUD OIG-issued hardware and software:

1. Protect HUD OIG's computer equipment and electronic media (portable disks and CD ROMs, thumb/flash drives or any other external hard drive) from damage, abuse, and unauthorized use.
2. Do not install/connect unauthorized hardware/software/firmware to the HUD OIG infrastructure. See Approved/Optional Hardware/Software List.
3. Do not make unauthorized configuration changes.
4. Do not connect non-HUD OIG-issued equipment to the HUD OIG network or any other HUD OIG resource, with the exception of personal computers to access MyPC.
5. Do not participate in the unlawful acquisition, use, reproduction, transmission, and/or distribution of computer software or media or other material protected by copyright laws, trademarks, or other intellectual property rights.
6. All electronic media used to transport HUD OIG business documents and data (flash drives, external hard drives, CD ROMs, etc.) must be encrypted with strong passwords to ensure protection of the data being transferred.
7. Ensure that data copied to flash drives, CDs/DVDs, and SD cards is also stored on a network drive. When network connectivity is not available and the local drive is used to store data, at first opportunity the data shall be copied to a network drive.
8. Make sure that critical information stored on your laptop or computer is also stored on your G: drive (personal) or H: Drive (shared).
9. Do not postpone unnecessarily the deployment of security patches to your HUD OIG computer(s). Save your documents and allow the installation of these patches as soon as possible.
10. Refer to the following Approved Hardware and Approved Software Lists

[Approved Hardware List](http://collaboration/sites/ask-it/documents/currentapprovedhardwarelist.pdf): <http://collaboration/sites/ask-it/documents/currentapprovedhardwarelist.pdf>

[Approved Software List](http://collaboration/sites/ask-it/documents/currentapprovedsoftwarelist.pdf): <http://collaboration/sites/ask-it/documents/currentapprovedsoftwarelist.pdf>

6. Teleworking

Employees who have approved for telework schedules at any alternate workplace must follow the following rules of behavior:

1. Follow security practices that are the same as or equivalent to those required at the primary workplace.
2. Physically protect any laptops or mobile devices used for teleworking when they are not in use.

HUD OIG OMT Rules of Behavior

3. Protect sensitive data at any alternate workplace. This includes disposing of sensitive information by shredding or other appropriate means.

7. Video Teleconference and Instant Messaging (IM) capabilities

As an authorized HUD OIG user, these are your responsibilities regarding the use of Instant Messaging and Teleconferencing:

1. Use HUD OIG IT equipment as designed. Do not alter the equipment or configuration; it is critical that the configuration be used as furnished, e.g., Roundtable camera(s) coupled to laptop(s) provided.
2. Request the use of additional equipment via the move, add, change (MAC) Add process in order to ensure interoperability and compliance with HUD OIG network security policies.
3. Do not use unauthorized, non-standard, or unapproved IM technology (i.e. Yahoo, MSN, G-Talk, etc.). Exception requests should be authorized by your manager and submitted to the HUD OIG Help Desk for implementation.
4. Only use videoconferencing services for business use and meetings that help HUD OIG conduct its day-to-day business and fulfill its missions.
5. Follow HUD OIG Policies, Federal Laws and Regulations when handling IM and video conference records.
6. Respect license and other agreements for videoconferencing and instant messaging services. No commercial gain by staff will be authorized.
7. Do not send or share confidential business information over IM.

8. Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information that could be used to distinguish or trace an individual's identity. Sensitive Data is any information that, through loss, unauthorized access, or modification, could adversely affect the National Interest, the conduct of Federal programs, or the privacy of individuals (which is protected under the Privacy Act), but that has not been specifically authorized (under criteria established by an Executive Order or an Act of Congress) to be kept secret.

In keeping with OIGM 1054, *Office Automation*, HUD OIG users are required to process, store, and transfer PII and Sensitive Data in a secure manner. As an authorized HUD OIG user, these are your responsibilities regarding the use and protection of Personally Identifiable Information:

1. Use PII only in ways applicable to your job duties and responsibilities, ensuring the protection of an individual's privacy.
2. Encrypt all PII and Sensitive Data stored on any equipment, including but not limited to external hard drives, mobile devices, CD-ROMs, and thumb/flash drives.
3. Do not store, process, transmit, and/or transfer PII and/or Sensitive Data on or to non-HUD OIG resources (e.g., forwarding to a non-HUD OIG email account, emailing data to

HUD OIG OMT Rules of Behavior

other investigative services, etc.) unless an approved encryption method is used and the transaction is documented/logged with the user's immediate supervisor.

4. Do not improperly alter or destroy PII or Sensitive Data.
5. Do not use PII or Sensitive Data in ways that are incompatible with the intended use.

Likewise, in accordance with OIGM 1054.2, *Breach Notification Response Plan*, immediately report all security breaches involving PII and Sensitive Data to the HUD OIG Duty Officer.

HUD OIG Duty Officer: **Phone:** (202) 708-5998

9. Disciplinary Actions

All HUD OIG personnel (including contractors) with access to HUD OIG resources shall follow the Rules of Behavior outlined in this document. Users are accountable for their actions and responsible for information security. Failure to follow these Rules of Behavior may result in disciplinary action. At the discretion of HUD OIG management, the penalty for noncompliance could include, but is not limited to: verbal or written warning; removal of system access; reassignment to other duties; demotion, suspension, or termination; and possible criminal and/or civil prosecution.

10. Acknowledgment Statement

I acknowledge that I have read the Rules of Behavior Version 8.0 dated April 2016. I further certify that I understand the information contained therein, and I will comply with the guidance and policy provided. I understand that I have no expectation of privacy when using HUD OIG resources (to include laptops, equipment, and networks) and that HUD OIG reserves the right to monitor all activity and collect information for system maintenance, validation, legal or any other lawful purposes without notifying me.

I understand that failure to comply with these rules could result in verbal or written reprimands, removal of HUD OIG network access, reassignment to other duties, criminal and/or civil prosecution, and/or termination of employment.

User Name (printed):

User Signature

Date