



# Information Security Acceptable Use Policy

## 1. Purpose

This policy establishes requirements for using and protecting HHS [information resources](#). Information resources include HHS data, [information systems](#), and equipment.

This policy also ensures that you are informed of and agree to your responsibilities concerning the use and protection of HHS information resources.

This policy supports requirements in the [Information Security Policy](#), [Circular-021: HHS Information Security/Cybersecurity Policy](#), [Texas Administrative Code, Chapter 202, Prohibited Technologies Security Policy](#), and all other relevant HHS, state, and federal policies and regulations.

## 2. Scope

This policy applies to all HHS desktop computers, laptops, [servers](#), [software](#), [data](#), [mobile devices](#), and any other HHS information resources that are connected to the HHS network or that process HHS data.

The scope of this policy includes equipment not owned by HHS, if it is used to access HHS data or information systems to perform HHS business.

## 3. Audience

This policy applies to you, if you are authorized to access HHS information resources; that is, if:

- You are an HHS workforce member, defined for the purposes of this policy as an HHS employee, intern, trainee, or volunteer.
- You are a [staff augmentation contractor](#).
- You or your employer or contracting entity are contracted to provide services to HHS or are an [external entity](#) that has an agreement with HHS to access HHS information resources.

This policy applies when you work in a state office or in another location, such as your home.

This policy excludes members of the public who use an HHS information resource to receive services from HHS.

## 4. Policy

### 4.1 Understanding Access

Use HHS information resources only for the purposes explicitly covered in this policy, unless you are explicitly granted permission to do otherwise by the proper information owner, laws and regulations, or contract.

As an authorized user, you must only use HHS information resources for HHS business purposes or for limited personal use. Limited personal use (for example, use of email or a web browser) is explained in Chapter 1, Section D, Standards of Conduct in the [HHS Human Resources Policy Manual](#).

#### **Prevent and Report Unauthorized Use**

Unauthorized access to or disclosure, duplication, modification, diversion, or destruction of HHS information resources is prohibited.

You must prevent unauthorized use of HHS information resources that you are authorized to use. Immediately report a suspected or known security incident or weakness to the HHS IT Customer Support Help Desk (Help Desk), per the HHS [Information Security/Cybersecurity](#) page.

Do not enter or change information in an HHS system or database without proper authorization, per [Chapter 33 of the Texas Penal Code](#).

## **The Consequences of Unauthorized Use**

Failure to comply with the requirements in this policy may result in disciplinary or corrective actions explained in the [HHS Human Resources Policy Manual](#).

If you disregard the security requirements explained in this policy, such as not taking the required training or not using the HHS network appropriately, the Chief Information Security Office may:

- Notify your manager, who will take the corrective or disciplinary actions explained in Chapter 1, Section F of the [HHS Human Resources Policy Manual](#), as appropriate.
- Require you to take training to help you understand the importance of security requirements and avoid future violations.

If you commit the following offences, you could be fined, incarcerated, or both:

- Access an HHS information resource without proper authorization.
- Give another party unauthorized access.
- Maliciously cause a computer malfunction.

## **4.2 Becoming an Authorized User**

### **4.2.1. Take the Required Training**

If you use HHS information resources, you must take the information security training that applies to you, even if you are not an HHS workforce member, as explained in the [Information Security Training, Awareness, and Continuing Education Policy](#).

### **4.2.2. Read and Complete the Acceptable Use Agreement**

Before you can access an HHS information resource for the first time, you must read this policy and complete the [Acceptable Use Agreement](#) to acknowledge that you understand and will comply with your obligations under this policy.

You may be asked to complete the Acceptable Use Agreement more than once (for example, each time you accept a new job at HHS).

You may be asked to complete the Acceptable Use Agreement in electronic format (such as on IAM Online or the Enterprise Portal), in print format, or both.

## **Workforce Members and Staff Augmentation Contractors**

If you are a new HHS workforce member or new staff augmentation contractor, your supervisor must:

- Ensure that you complete and sign the Acceptable Use Agreement in electronic or print format during the hiring or contracting process.
- Retain a copy of your Acceptable Use Agreement.
- **Workforce members only:** Send a copy to HHS Human Resources.

## **Employees of Contractors and Other External Entities**

If you work for an external entity and are not a staff augmentation contractor, your assigned HHS contract manager must:

- Ensure that you complete and sign the Acceptable Use Agreement electronically or in print format, when you are hired.
- Retain a copy (for example, in a contract file), if you sign the Acceptable Use Agreement outside of the HHS Enterprise Portal. (The portal retains a record.)

### **4.2.3. Maintain Your Authorization**

After you sign the Acceptable Use Agreement, you will receive an annual reminder of your obligations under it, along with instructions to review this policy for updates. You must stay up to date on changes to the policy to retain your authorized access.

### **4.2.4. Have No Expectation of Privacy**

When using HHS information resources, you must have no expectation of privacy, even when accessing HHS information resources from a device not owned by HHS. HHS may monitor your use of HHS information resources at any time and on any device. By using HHS information resources, you consent to being monitored.

Without notification, HHS may:

- Make subject to [electronic discovery](#) any information that you have stored in or that is associated with an HHS information resource (including personal email, voicemail, files, or messages).
- Review and provide the information for open records requests, legislative requests, litigation purposes, and investigations.

To protect your privacy and to protect against loss of personal information, avoid storing personal information on HHS information resources, particularly large files.

#### **4.2.5. Receive Access**

You will only receive access to the HHS information resources (electronic and print) that you need to perform your essential job functions, and you will be granted the least amount of access sufficient to perform those functions.

#### **Confidential or Sensitive Information**

If your essential job functions require access to information that is [confidential](#) or [agency sensitive](#), you may be required to complete other documentation or training, in addition to reading and signing the Acceptable Use Agreement.

#### **4.2.6. Set Up Your User Credentials**

After you receive access to HHS information resources, you must set up your credentials by creating a [strong password](#) and user name, if needed.

You must use your own assigned credentials to access HHS information resources.

Never write down or store your password. If needed, use one of the approved password managers listed in the [Software Catalog](#). Never use a Remember Password or auto logon feature, except on approved IT-managed systems.

Never reveal your password to anyone, including administrative assistants, management, or the Help Desk.

Actions initiated under your credentials are considered to be authorized and electronically signed by you.

If you suspect that your account or password is compromised, you must:

- Immediately change your password and then report it to the [Help Desk](#).
- Follow the Help Desk's instructions to secure your account.

### **4.3 Accessing HHS Resources**

When outside of the US or its territories, you must not access any HHS information resources owned by HHS or an HHS third-party vendor from any device using any type of network connection (wireless or physical). Such access is high risk.

#### 4.3.1. Use Software Appropriately

You must use only HHS-approved and properly licensed software to access HHS information resources. Follow all requirements in the [Software Policy](#) and the [Prohibited Technologies Security Policy](#).

Approved software, including mobile applications, are listed in the [Software Catalog](#). Prohibited software is also listed, to help you know not to use it.

You must not disable or bypass malware protection software, unless you are doing so as part of your assigned job functions, and with the approval of both your manager and the HHS Chief Information Security Office.

Always follow applicable copyright laws when using HHS information resources.

#### 4.3.2. Use the Network Appropriately

Do not modify hardware or settings to extend network capabilities. For example, you are prohibited from using or installing a device such as a wireless router on the HHS network. If you have a business need for such a device, your supervisor must submit a [Help Desk](#) ticket to get appropriate approval. This is not the same as using a home or non-HHS wireless network to connect to the HHS network with approved VPN software, which is permitted per section [4.3.4](#).

As explained in the [Prohibited Technologies Security Policy](#), unless you have an approved exception per the policy:

- Do not connect to an HHS network using a device that has prohibited technology on it.
- Do not attempt to download or install a prohibited technology on a device while it's connected to an HHS network.

#### Confidential or Sensitive Information

To ensure that agency sensitive or confidential information, including electronic protected health information, is protected:

- Follow the guidelines in the [Data Classification Standard](#).
- Refer to the HHS Approved Hardware List on the [Requesting Hardware and Software](#) page.

Never use chat or text messages to send confidential information.

Never circumvent security policies for internet browsing (for example, by using personal or publicly available proxy servers or devices).

#### **4.3.3. Follow Communication Requirements**

You must follow all applicable requirements for communication in Chapter 1, Section D, Standards of Conduct, in the [HHS Human Resources Policy Manual](#).

#### **Social Media**

You must follow the guidance in [Circular-042: HHS Social Media Policy](#) and Chapter 1, Section D.14 of the [HHS Human Resources Policy Manual](#) to determine when you can use social media.

Unless you have an approved exception, you must not use social media if it is prohibited by the [Prohibited Technologies Security Policy](#). For information on exceptions, see the policy.

#### **Email**

Do not open email attachments or links from unknown senders. Emails from senders external to HHS are identified by a banner.

Do not send unsolicited messages to large groups, except as required to conduct HHS business.

#### **Confidential or Sensitive Information**

To send confidential information by email, you must follow the requirements in [4.3.9](#) and in the [Data Classification Standard](#).

Do not use your HHS email account to send confidential or agency sensitive information to your personal email account (such as a personal Gmail or Outlook account), unless it's your information (such as your tax documents or documents related to your compensation, severance, or retirement plans and benefits).

Do not use your personal email account to:

- Send HHS information that is confidential or [agency sensitive](#).
- Receive HHS information that is [confidential](#) or agency sensitive (including from your HHS email account).
- Conduct HHS business.

## **Instant Messaging and Collaboration in Microsoft Teams**

Use Microsoft Teams for instant messaging. Teams is HHS's standard instant messaging software.

As an authorized user, you may give another user control of a Teams meeting, but you are responsible for that user's actions, as explained in the [Microsoft Teams Policy](#).

When using Teams, you must follow all requirements in the [Microsoft Teams Policy](#).

### **4.3.4. Request Remote and VPN Access**

To request VPN remote access to the HHS network, you must get your supervisor's approval, per the HHS [Remote Access](#) page.

If you are authorized to telework or to access HHS information resources from equipment not owned by HHS using remote access technology (for example, the Outlook Web access link), you must follow security practices that are equivalent to those required at your primary workplace, per the guidance on the HHS [Pay, Benefits and Telework](#) page and in [4.3.5](#) of this policy.

If you use HHS VPN, you must obtain your own internet service provider.

VPN automatically disconnects after a time predetermined by HHS. Maintaining an inactive connection to any technology (using Ping, StayConnect, and so on) is prohibited and may result in termination of your VPN account.

Only authorized workforce members can use remote desktop assistance to remotely access and control someone else's computer as part of their essential job functions.

### **4.3.5. Use Laptops, Desktops, Mobile Devices, and Printers**

Unless you have an approved exception, you must follow the requirements in the [Prohibited Technologies Security Policy](#), as they pertain to your devices:

- Do not use prohibited technology on an HHS owned or issued device.
- Do not use a personally owned device with prohibited technology on it to access HHS information resources.
- Do not use a personally owned device to record, capture, or share agency sensitive or confidential information.

For additional information, including which technologies are prohibited and how to request exceptions, see the policy.

Follow any other requirements that apply to your device, as explained below.

If you choose to use a personal device for state business, you are responsible for any associated costs.

## **Mobile Devices**

Follow the requirements in the [Using a Mobile Device to Access HHS Data Policy](#) to appropriately use an HHS-issued or personal [mobile device](#).

For personal mobile devices, ensure that you follow the requirements explained on the [Personal Wireless Device](#) page and comply with all HHS security policies, standards, and controls.

For information on how to request an HHS mobile device, see the [State-Issued Wireless Telecommunication Equipment or Service Policy and Procedure](#).

## **Laptop and Desktop Computers**

Follow the requirements in the [Computing Devices and Accessories Policy](#) to request an HHS laptop or desktop computer.

If you use a laptop or desktop computer not owned by HHS to access HHS information resources, you must use approved software to make the remote connection (such as agency-approved VPN software) or use Microsoft 365 services.

## **Printers**

Use only HHS-owned and issued printers to print work-related documents. This includes printing from an approved telework location, such as your home.

### **4.3.6. Protect HHS Information**

HHS information resources must be protected according to the requirements in the [Data Classification Standard](#).

If you are aware of or suspect a security incident, a security weakness, misuse of HHS information resources, or a violation of any policy related to the security and protection of HHS information resources, you must:

- Immediately report the incident to the [Help Desk](#).

- Follow their instructions to identify and [remediate](#) the incident.

#### **4.3.7. Dispose of HHS-Owned Media Appropriately**

You must properly dispose of (purge and destroy) digital media.

Digital media includes software, digital images and video, web pages and websites, digital data and databases, electronic documents, and digital audio such as MP3.

When using digital media, you must follow the media sanitization procedures in [Information Security Controls](#), Media Protection (MP-01), and in the [Data Classification Standard](#).

If you need help disposing of the media, contact the [Help Desk](#).

Before disposing of digital media, releasing it from HHS control, or releasing it for reuse, you must sanitize it using the techniques required by the resources listed in [5.1 Federal and State Requirements](#).

You must dispose of physical media, such as CDs and DVDs, according to the requirements in the [Data Classification Standard](#).

#### **4.3.8. Maintain Physical Security and Control**

Before using, disclosing, transmitting, maintaining, or creating HHS information resources (including confidential and agency sensitive information), you must obtain proper authorization and approval from your supervisor.

When removing HHS information resources (including confidential and agency sensitive information) from HHS property, you must follow the same information security policies, standards, controls, and guidelines to protect the resource, as required when using the resource at an HHS location.

To protect HHS information resources from damage, loss, or theft, you must keep them secured and under your physical control at all times and follow the safeguards explained in this policy.

#### **Loss or Theft**

If your device is lost or stolen and HHS issued it to you, or you used it to access HHS information resources, you must follow the [Reporting a Lost or Stolen Device Process](#) to file a report with the Help Desk.

#### **4.3.9. Protect HHS Confidential Information**

You must follow the [Data Classification Standard](#) when handling, processing, or managing HHS information in electronic or print format.

##### **Encryption**

Confidential and agency sensitive information must be encrypted using an HHS-approved encryption technology, per the [Data Classification Standard](#).

##### **Password Protection**

All HHS portable or removable media (such as tablets and flash drives) containing confidential information must be password protected and encrypted with an approved [FIPS 140-2](#) cryptographic module.

##### **Unauthorized Viewing**

When using a computer to view sensitive or confidential information, you must position it to prevent unauthorized viewing or access.

##### **Key Cards**

Immediately upon becoming aware that a keycard is lost or stolen, report it to the appropriate facility manager.

Do not:

- Leave keys used to access confidential or sensitive information unattended.
- Distribute, copy, loan, or share a keycard or other access mechanism, unless doing so is part of your specific job functions.

When you no longer need a keycard or other access mechanism, you must return it to the office or area that issued it.

##### **IRS Federal Tax Information**

If you suspect any of the following, file an incident report immediately (before 24 hours has elapsed) with the HHS [IRS coordinator](#):

- An unauthorized person has accessed federal tax information (FTI).
- An authorized person has disclosed FTI to an unauthorized person or accessed FTI without a need to know (that is, without a business reason).

- An authorized person has printed FTI, or downloaded, copied, or saved FTI to another location. These actions make FTI more susceptible to unauthorized access.

If the reported action is an incident, the IRS coordinator notifies HHS Privacy. Privacy investigates by taking the steps explained in [Circular-057: Protecting Confidential Information and Responding to Privacy Breaches](#) and the Privacy Incident Response Plan, notifies the appropriate contacts, and responds to the incident according to the requirements in [IRS Publication 1075](#).

In some cases, an incident may be both a privacy and an information security incident. In such cases, the [Information Security Incident Response Policy](#), [Information Security Incident Response Process](#), and Information Security Incident Response Plan also apply.

## **Loss or Theft**

As a proactive measure, you must be prepared, at a minimum, to describe the agency sensitive or confidential information on a device that you are in possession of, in case the device is lost or stolen.

If the device is lost or stolen, you must follow the [Reporting a Lost or Stolen Device Process](#) to file a report with the Help Desk. When making your report, describe the agency sensitive or confidential information on the device.

Also report the loss or theft of agency sensitive or confidential information to:

- Your supervisor or manager.
- The chief information security officer, and other agency or HHS offices as applicable, as explained in the [Information Security Incident Response Policy](#).
- The [HHS Privacy Division's Incident Response team](#), per the instructions on the [HHS Privacy Division's](#) page and in [Circular-057: Protecting Confidential Information and Responding to Privacy Breaches](#).

## **5. Related Resources**

Some resources are restricted to people with access rights.

## **5.1 Federal and State Requirements**

### **Federal Information Processing Standard (FIPS) 140-2**

Specifies the security requirements that must be satisfied by a cryptographic module.

### **Texas Administrative Code, Chapter 202, Information Security Standards**

Establishes the information security standards followed by state agencies in Texas.

### **Texas Penal Code, Title 7, Chapter 33, Computer Crimes**

Defines Texas law related to securing computers and data.

### **IRS Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies**

Explains the security guidelines for protecting federal tax returns and tax return information.

## **5.2 Policies and Standards**

### **HHS Human Resources Policy Manual**

Establishes requirements for employment, benefits, leave, and compensation.

### **Circular-021: HHS Information Security/Cybersecurity Policy**

Explains how HHS protects HHS information resources.

### **Information Security Policy**

Provides a framework for the protection of HHS information resources.

### **Data Classification Standard**

Communicates the required protections for HHS information resources.

### **Information Security Controls**

Explains the safeguards and countermeasures needed to satisfy information security requirements.

### **Circular-042: HHS Social Media Policy**

Establishes clear standards and responsibilities for the use of social media tools to increase awareness of state programs and services according to state law, codes, and HHS policies and procedures.

### **Software Policy**

Establishes requirements for software used within the HHS system, including requirements related to requesting, licensing, installing, removing, auditing, and tracking software.

### **Information Security Incident Response Policy**

Establishes requirements for reporting, prioritizing, and handling information security incidents involving HHS information resources.

### **Information Security Training, Awareness, and Continuing Education Policy**

Establishes information security training, awareness, and continuing education requirements to protect HHS.

### **Microsoft Teams Policy**

Establishes requirements for the use of Microsoft Teams for the HHS system.

### **Circular-057: Protecting Confidential Information and Responding to Privacy Breaches**

Establishes the HHS policies for safeguarding confidential information and reporting and responding to privacy breaches.

### **Using a Mobile Device to Access HHS Data Policy**

Establishes HHS acceptable use, maintenance, and security requirements for mobile devices that are used to access HHS data.

### **Computing Devices and Accessories Policy**

Establishes requirements for HHS issued laptop and desktop computers and their accessories, such as how to request or return them.

### **Prohibited Technologies Security Policy**

Establishes the technologies that are prohibited by the Governor of Texas or DIR and the measures HHS is required to take to prevent their use.

### **State-Issued Wireless Telecommunication Equipment or Service Policy and Procedure**

Establishes eligibility and other requirements for state-issued mobile phones.

## **5.3 Processes and Procedures**

### **Information Security Incident Response Process**

Establishes the requirements for reporting, prioritizing, and handling information security incidents that involve HHS information resources.

### **Reporting a Lost or Stolen Device Process**

Explains how to report a device as lost or stolen if it can be used to access HHS information and what actions are taken when a report is made.

## **5.4 Definitions and Other**

### **HHS Acceptable Use Agreement**

Informs authorized users of their responsibilities when using HHS information resources.

### **HHSC Software Catalog**

Catalog of software approved for use by authorized users.

### **Information Security Incident Response Plan**

Confidential internal procedures used to respond to security incidents.

### **Privacy Incident Response Plan**

Confidential internal procedures used to respond to privacy incidents.

### **IT Glossary**

Provides definitions for technical or specialized terms.

## 6. Revision History

Published	Effective	Change Type	Change Summary	Owner
04/28/2023	04/28/2023	Revised	<a href="#">Read change summary</a>	Chief Information Security Office
02/15/2023	02/15/2023	Revised	<a href="#">Read change summary</a>	Chief Information Security Office
06/23/2022	06/23/2022	Revised	<a href="#">Read change summary</a>	Chief Information Security Office
8/13/2021	8/13/2021	Revised	<a href="#">Read change summary</a>	Chief Information Security Office
7/15/2015	7/15/2015	Issued	N/A	Chief Information Security Office

### Request Revisions

For revisions to this document, submit a [request form](#).