

## ACCEPTABLE USE OF COMPUTERS AND INFORMATION TECHNOLOGY RESOURCES

### 9.31.0 INTRODUCTION

#### 9.31.0-1 Policy Statement

This policy establishes responsibilities for acceptable use of the County of Houston information technology resources. County information technology resources are provided for use by the Board of Commissioners, other elected officials, employees and other authorized users. County information technology resources are the property of the County of Houston and are provided for the support of the County's business purposes. The use of County information technology is conditioned on compliance with this policy and related County Regulation 9.30.1 Cellular and Mobile Computing Devices, and any procedures or guidelines adopted by the County.

Computer and information technology resources are essential tools in accomplishing the mission of the County of Houston governmental divisions. These resources must be used and managed responsibly in order to ensure their availability for the competing demands of mission-related uses. This policy establishes responsibilities for acceptable use of the County of Houston information technology resources. As such, the County encourages the use of information technology as an effective and efficient tool within the framework of applicable state and federal laws, policies and rules.

#### 9.31.0-2 Applicability/Scope

This policy applies to all users of County information technology, wherever located. The County Board has adopted operational procedures within, including, but not limited to: security; employee use, monitoring, unauthorized uses and other limitations on use consistent with federal and State of Minnesota law, the Houston County Code of Ethics and the County's Data Practices Policy and Compliance Manual.

The County of Houston is not responsible for any personal or unauthorized use of its resources.

#### 9.31.0-3 Definitions

The definitions in HC Regulation 9.31, apply to HC Regulation 9.31 Cellular and Other Mobile Computing Devices. The definitions set forth in HC Regulation 9.31 are also incorporated into this policy regulation.

**County** – means the Board of Commissioners and Department Heads when acting in their official capacities on behalf of the governmental divisions of Houston County.

**County Information Technology** - means all County facilities, technologies, and information resources used for information collection, processing, transfer, storage and communications. This includes, but is not limited to, computer hardware and software, electronic communications devices and services, such as modems, e-mail, networks, telephones, voicemail, voice over

internet connections, facsimile transmissions, video, cameras, mobile computing devices, printers and multimedia materials.

**Security Measures** -measures means processes, software, and hardware used by County network administrator(s) to protect the confidentiality, integrity, and availability of the computer resources and data owned by the County or its authorized users. Security measures may include, but are not limited to, monitoring or reviewing individual user accounts for suspected policy violations and investigating security-related issues.

**Transmit** means to send, store, collect, transfer or otherwise alter or affect information technology resources or data contained therein.

**User** -means any individual, including, but not limited to, elected officials, employees, interns, volunteers, and other authorized individuals using County information technology in any manner, whether or not the user is affiliated with County.

## 9.31.1 RESPONSIBILITIES OF ALL USERS

### 9.31.1-1 Compliance with Law and County Policies

- Users must comply with federal and Minnesota state laws, County policies, County contracts and licenses applicable to their particular uses. This includes, but is not limited to laws related to: libel, data privacy, copyright, trademark, gambling, obscenity, and child pornography; the federal Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit hacking and similar activities; Minnesota state computer crime statutes.
- Users are responsible for the content of their personal use of County information technology and may be subject to liability resulting from that use.
- Users must use only County information technology they are authorized to use and use them only in the manner and to the extent authorized and for which they have a legitimate business purpose. Ability to access information technology resources does not, by itself, imply authorization to do so.
- Users are responsible for use of County information technology under their authorization.

### 9.31.1-2Unauthorized Use

Users must abide by the security restrictions on all systems and information to which access is authorized.

- Users must not allow others who are not authorized to:
  - use any account or password assigned by the system to anyone else;
  - share any account or password, assigned to the user by the County, with any other individual, including family members; and
  - to use County information technology under the user's control.

- Users must not circumvent, attempt to circumvent, or assist another in circumventing security controls in place to protect the privacy and integrity of data stored on County information technology.
- Users must not change, conceal, or forge the identification of the person using County information technology, including, but not limited to, use of e-mail.
- Users must not knowingly download or install software onto County information technology without prior authorization from the County Director of Information Technology. The County reserves the right to remove unauthorized software at anytime and without prior notice.
- Users must not engage in activities that interfere with or disrupt network users, equipment or service; intentionally distribute viruses, worms, Trojans, or other malicious code; or install software or hardware that permits unauthorized access to system information technology.
- Users must not engage in inappropriate uses, including:
  - Activities that violate state or federal law or regulation;
  - Wagering or betting;
  - Harassment, threats to or defamation of others, stalking, and/or illegal discrimination;
  - Fund-raising, private business, or commercial activity, unless it is related to the mission of the County agency. Mission related activities are determined by the Board of Commissioners or individual Department Head;
  - Storage, display, transmission, or intentional or solicited receipt of material that is or may be reasonably regarded as obscene, sexually explicit, or pornographic, including any depiction, photograph, audio recording, video or written word, except as such access relates to the professional activities of an employee.
  - Spamming through widespread dissemination of unsolicited and unauthorized e-mail messages.

### **9.31.1-3 Protecting Privacy**

Users must not violate the privacy of other users regardless of whether those accounts are securely protected. Technical ability to access others accounts does not imply authorization to do so.

### **9.31.1-4 Union Activities**

- In the interest of maintaining effective labor-management relationships and efficient use of County time and resources, County e-mail accounts may be used by employee representatives of the union for certain union activities, in accordance with County policy, state law and/or the provisions of applicable collective bargaining agreements.

- County-owned property or services, including the e-mail system, may not be used for political activities, fund-raising, campaigning for union office, union organizing activities, or solicitation of employees for union membership.
  - Union use of County electronic communication technology, as authorized, is subject to the same conditions as employee use of such technology.

**9.31.1-5 Political Activities**

County employees shall not use County information technology for political activities.

**9.31.1-6 Religious Activities**

County employees shall not use County information technology in a manner that creates the impression that the County supports any religious group or religion generally in violation of the Establishment Clause of the First Amendment of the United States Constitution or Article 1, Section 16 of the Minnesota State Constitution.

**9.31.1-7 Personal Use Limitations**

Users must avoid excessive personal use of system information technology including any personal usage that interferes with network capacity or others' authorized use. Users shall refrain from streaming audio or video that is not related to performing professional duties. The reasonableness of any specific use shall be determined by the Department Head in context of relevant circumstances.

- County employees may make reasonable use of County information technology for personal communications as long as the use is in accordance with state law, Houston County regulations and policies; and the use, including the value of employee time spent, does not result in an incremental cost to the County, or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impracticable, as determined by the County. Reasonable use means use consistent with this policy.
- Employees who use County technology systems for personal use have **no expectation of privacy** when using in any information that is stored or transmitted by use of any County information technology and may be monitored by the County in compliance with this and other County policies.
- Employees will reimburse the County for the personal use of County copy and facsimile machines for personal use at the same rate that is required of the citizens of the County.

*\*\*\*Personal use of County-owned cellular devices is not allowed. See HC Policy 9.31 Cellular and Other Mobile Computing Devices.*

## 9.31.2 DATA RETENTION AND SECURITY

### 9.31.2-1 Government Data Practices and Records Laws

Security of data transmitted on its information technology resources cannot be fully guaranteed. Therefore, data transmitted via County information technology are not guaranteed to be private and deletion of a message or file may not fully eliminate the data from the system.

Government data maintained on County information technology is subject to the Minnesota Government Data Practices Act (MGDPA), to the same extent as they would be if kept in any other medium. Users are responsible for handling government data to which they have access or control in accordance with applicable data practices laws. Therefore, users should exercise caution when determining to transmit data classified as private, confidential or non-public as defined by the MGDPA and employ reasonable physical and technological security measures to protect County records in all phases of handling. This may include, but is not limited to, the appropriate use of secure facsimiles or encryption or encoding devices when electronically transmitting data that is not public.

### 9.31.2-2 Right to employ security measures

The County reserves the right to employ security measures, including but not limited to, the right to monitor any use of system information technology, including those used in part for personal purposes. Users have no expectation of privacy for any use of system technology resources, except as provided under federal wire tap regulations (21 U.S.C. Sections 2701-2711).

- Normal operation and maintenance of County information technology may require periodic monitoring and regular trouble-shooting for network integrity and data security, backup and caching of data and communications and the logging of activity. County officials may access data on system information technology, without notice, for business purposes including, but not limited to, retrieving business-related information; re-routing or disposing of undeliverable mail; or responding to requests for information permitted by law.
- Employees should immediately report all concerns of violation of this policy to their supervisor or Department Head. The Department Head or supervisor, will consult with the Human Resource Director regarding the reported concern. The Human Resources Director may further consult with the Director of Information Systems to investigate and recommend corrective action or other actions as warranted.
- Concerns involving a potential risk of harm to the integrity or security of the Houston County information systems shall be immediately reported to the Director of Information Services by all employees.

**NOTICE:** The concerns you report may contain information that is classified by the Minnesota Government Data Practices Act as “Confidential” or “Private”, thus only those persons with a “business purpose” have access to such information. Therefore, employees shall not share their concerns with others individuals except as set forth in this policy.

**9.31.2-2 Records Retention**

The County’s retention schedule applies to all government data, which is stored on the County’s technology systems. The County’s retention schedule applies to electronic data in the same manner as other recorded data.

**9.31.3 SANCTIONS**

**9.31.3-1 Access Limitations**

The County of Houston reserves the right to temporarily restrict or prohibit use of its County information technology by any user without notice, if it is determined necessary for County government business purposes.

**9.31.3-2 Disciplinary proceedings**

Alleged willful or intentional violations shall be addressed through applicable County policy and procedures and/or appropriate collective bargaining agreement. Users who violate this policy may be denied access to County information technology and may be subject disciplinary action. Discipline for violations of this policy may include any action up to and including termination.

**9.31.3-3 Referral to Law Enforcement or other Agencies**

Under appropriate circumstances, the County of Houston may refer suspected violations of law to appropriate law enforcement authorities or other state or federal agencies, and provide access to investigative or other data as permitted by law.

**9.31.0-64 Questions Regarding This Policy**

Employees who have questions about this policy may present their questions to their department head or supervisor, the Director of Information Systems or the Director of Human Resources.

---

**Related County Documents:**

[HC Policy 9.20 Employee Code of Ethics](#)

[HC Policy 9.31 Cellular and Other Mobile Computing Devices](#)

[HC Policy 9.29 Data Practices Policy and Compliance Manual](#)

[HC Policy 9.40 Report/Complaint of Discrimination/Harassment Investigation and Resolution](#)

---

**Authenticated by:**

**Laurence Connery  
Houston County Board Chair**

***Date of Adoption:*** 2004

***Date & Subject of Revisions:*** September XX, 2010