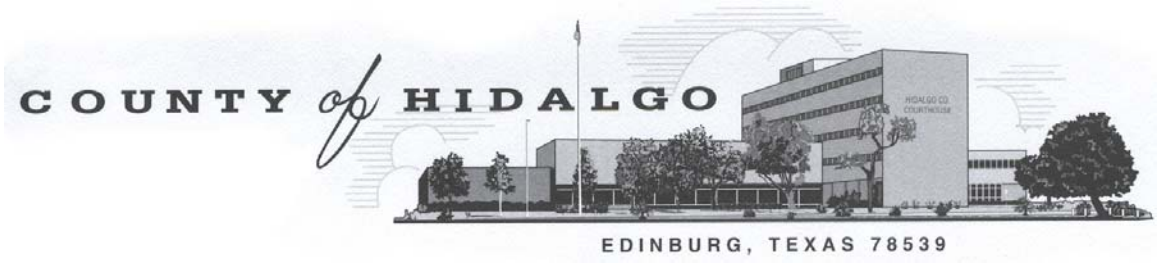
COUNTY of HIDALGO

EDINBURG, TEXAS 78539

Information Technology Security Policies

TABLE OF CONTENTS



POLICY CHECKLIST

#	Policy Name	Required	Published	Approved	Revised
1	Acceptable/Unacceptable Use	YES	YES	YES	10/02/03
2	Account Management	YES	YES	YES	04/20/04
3	Admin/Special Access	YES	YES	YES	04/20/04
4	Change Management	YES	YES	YES	04/20/04
5	Disaster Recovery	YES	YES	YES	04/20/04
6	Incident Management	YES	YES	YES	04/20/04
7	Network Configuration	YES	YES	YES	04/20/04
8	Password	YES	YES	YES	04/20/04
9	Physical Access	YES	YES	YES	04/20/04
10	Privacy	YES	YES		
11	Security Training	YES	YES	YES	04/20/04
12	Software Licensing	YES	YES	YES	04/20/04
13	Virus Protection	YES	YES	YES	04/20/04

Introduction: Network and data computer systems and infrastructure are meant to be used to grant access to Hidalgo County Information Resources. These resources provide a means of providing access to information and accountability of said access. This accountability is the key to any computer security program, for Information Resources usage. This means that creating, controlling and monitoring all Information Resources is extremely important to the overall security program.

Purpose: To ensure that its Information Resources are used properly by its employees, independent contractors, agents and other computer users, Hidalgo County has created these Information Technology Security Policies. The purpose of these policies is to establish rules for the creation, monitoring, control and removal of access to all Information Resources.

Audience: The rules and obligations described in this Policy apply to all users of Hidalgo County's computer network, wherever they may be located. Violations will be taken very seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

Definitions: **Information Resources (IR):** The term "Information Resources" refers to Hidalgo County's entire computer network, equipment, data and related peripherals. Specifically, Information Resources includes any and all computer printouts, online display devices, magnetic storage media and all computer-related activities involving any device capable of receiving email, text messaging, messaging, blogging, posting on public social networking sites, browsing internet sites or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to: Mainframes, servers, GPS tracking devices, GIS equipment, mobile phones, personal computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), audio visual equipment, telecommunication resources, network environments, telephones, fax machines, printers, service bureaus and any future technology that may arise. Additionally, it is the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit information.

Chief Information Officer (CIO): Responsible to the County of Hidalgo County, Texas for management of the agency's information resources. This designation is intended to establish clear accountability of setting policy for information resources management activities, is responsible for the security of the resources, provide for greater coordination of the county's information activities and ensure greater visibility of such activities within and between state agencies. The CIO has been given authority and the accountability by the County of Hidalgo, Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the agency.

System Administrator: Person responsible for the effective operation and maintenance of specific departmental Information Resources, including implementation of standard procedures and controls to enforce the county's security policy. Because of statutory limitations and department specific responsibilities, the following departments within the County have System Administrators that report directly to the appointed official or elected official, and not the CIO: County Auditor, Sheriff's Office, District Attorney, Health Department and Tax Office.

These System Administrators are bound by these policies in their respective systems and applications.

User: Person who is the end client for an application on an information system. The user neither owns the IR resource or the data. Generally a user is any County department and/or elected office employee with access to a computer, who is neither IR system administrator, part of the IT staff, elected official or department head.

Policy 1.00 – Acceptable Use Policy

The computer system is the property of Hidalgo County and may be used only for legitimate business purposes. Users are permitted access to the computer system to assist them in the performance of their jobs. All users have the responsibility to use computer resources in a professional, ethical, and lawful manner. Use of the computer system is a privilege that may be revoked at any time.

A. Acceptable Use

Acceptable Use. Acceptable computer information systems use is limited to the following:

1. Incidental communication among Hidalgo County authorized users and professional colleagues which facilitates work assignments and professional development or debate in a work-related field of knowledge.

A. Communication with professional associations, governments, universities, businesses and/or individuals associated with the facilitation of County business, research and education efforts as authorized by the Department Head/Elected Official.

B. Distribution of information to the general public whereby such information is made available under the county guidelines and policies for the release of information and the Freedom of Information Act.

C. Only the TCP/IP protocol is permitted with the following services: WWW, POP3, IMAP, FTP, HTTPS, SMTP & SMNP. Additional protocols will be permitted if approved by the Chief Information Officer.

Unacceptable Use

A. Personal use not related to the conduct of work on behalf of Hidalgo County or other organizations as set forth in agreements and contracts with Hidalgo County.

B. To gain unlawful access to information or computer and communication resources.

C. Intentional introduction of, or experimentation with, malicious code including but not limited to computer worms or viruses.

D. Illegal, fraudulent or malicious activity; political activity; religious promotion; or activity on behalf of organizations or individuals having no affiliation with Hidalgo County.

E. Transmission of material in violation of applicable copyright laws or patents, including, but not limited to music, movies and software.

F. Pornographic material or content that could be found to be offensive.

G. Purchase and downloading of copyrighted material using the County's network. This refers specifically to online content stores.

H. The intentional sending of messages that is likely to result in the loss of recipient's work or system and any other types of use which could cause congestion including, but not limited to the network or otherwise interfere with the work of others.

I. Generation, storage, transmission or other use of data or other matter which is abusive, profane, or offensive to a reasonable person.

J. Generation, storage, transmission of confidential or otherwise non public information on County owned mobile devices (laptops, phones, PDAs, etc.) without proper safeguards such as passwords, encryption or security keys.

K. Passwords used to gain access to non-County Internet sites must not be the same passwords used on any Hidalgo County computer system.

Policy 2.00 - Account Management Policy

- All accounts created must have an associated request and approval from the IR systems administrator for the Hidalgo County system or service.
- All users are subject by the Hidalgo County Information Technology Privacy Policy once access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name. (i.e. *username.userlastname*)
- All default passwords for accounts must be constructed in accordance with the Hidalgo County Password Policy.
- All accounts must have a password expiration that complies with the Hidalgo County Password Policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- System Administrators or other designated staff:
  - are responsible for removing the accounts from the system they manage, of individuals that change roles within Hidalgo County or are separated from their relationship with Hidalgo County
  - must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
  - must have a documented process for periodically reviewing existing accounts for validity
  - are subject to independent audit review
  - must provide a list of accounts for the systems they administer when requested by authorized Hidalgo County management
  - must cooperate with authorized Hidalgo County management investigating security incidents.

Policy 3.00 – Admin/Special Access Policy

- All Hidalgo County departments and agencies must submit to IT a list of administrative contacts for their systems that are connected to Hidalgo County information resources.
- All users of Administrative/Special access accounts must be authorized by the IR system administrator.
- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must not engage in investigations. All requests for investigations must be processed according to the INCIDENT MANAGEMENT POLICY.
- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet the Hidalgo County Password Policy.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or Hidalgo County.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
  - must be authorized by the IR system administrator
  - must be created with a specific expiration date
  - must be removed when work is complete

Policy 4.00 – Change Management Policy

- Every change to a Hidalgo County Information Technology resource such as: operating systems, computing hardware, networks, and applications are subject to the Change Management Policy and must follow the Change Management Procedures.
- All changes and request for changes affecting computing environmental facilities (e.g., air-conditioning, security devices, all monitoring devices, cameras, phone systems, building additions or remodeling, electricity, and alarms) must be reported to the IR system administrator, department head / Elected Official and the CIO.
- A formal written change request must be submitted for all changes, both scheduled and unscheduled, to IR system administrator and the CIO.
- All scheduled change requests must be submitted to the IR system administrator and the CIO, in order to timely review the request, determine potential failures and make the decision to allow or delay the request.
- The IT Department may ask to delay a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year end accounting, it will affect overall network security or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- User notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to: Date of submission and date of change
  - Owner and custodian contact information
  - Nature of the change
  - Indication of success or failure
- All County of Hidalgo, Texas information systems regardless of the department where the system is, must comply with an Information Resources change management process that meets the standards outlined above.
- Users may not install unauthorized software or hardware on without prior approval of the IT Department.

Policy 5.00 – Backup / Disaster Recovery Plan (DRP)

- The frequency and extent of backups must be in accordance with the importance of the information on the system and the acceptable risk as determined by the data owner.
- All System Administrators must keep and maintain a Disaster Recovery Plan for their assigned system.
- The Hidalgo County information resources backup and recovery process for each system must be documented and periodically reviewed by the IR system administrator and submit a copy to the CIO.
- In case there is a vendor(s) providing offsite backup storage for Hidalgo County must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest Hidalgo County sensitivity level of information stored.
- Backups must be periodically tested to ensure that they are recoverable.
- Signature cards held by the offsite backup storage vendor(s) for access to Hidalgo County backup media must be reviewed annually or when an authorized individual leaves Hidalgo County.
- Procedures between Hidalgo County and the offsite backup storage vendor(s) must be reviewed at least annually.
- Backup tapes should have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
  - System name
  - Creation Date
  - Sensitivity Classification [Based on applicable electronic record retention regulations.]
  - Hidalgo County Contact Information.

Policy 6.00 – Incident Management Policy

- Whenever a security incident, such as a inappropriate content, copyrighted material, virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed the Incident Management procedures must be followed:
- The department user is responsible for notifying the IR system administrator, department head / elected official of that department so as to initiate the appropriate incident management action including restoration as defined in the Incident Management Procedures. The user may contact the CIO directly.
- The department head / elected official of that department are responsible for notifying the CIO.
- The CIO is responsible for determining the physical and electronic extent of the incident and will determine the need of an investigation of the incident. The CIO is responsible for coordinating communications with outside organizations and law enforcement.
- The IT Department can at any time remove access from any user as it deems appropriate for the overall benefit of the entire county wide IT infrastructure.
- The appropriate technical resources from the IT department are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The CIO and IT department will determine if a widespread Hidalgo County communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the IT Department are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

  The IT department is responsible for initiating, completing, and documenting the incident investigation as reporting the incident to:

  - Local, state or federal law officials as required by applicable statutes and/or regulations
- In the case where law enforcement is not involved, the CIO will recommend disciplinary actions, if appropriate, to the elected official or department head.

Policy 7.00 – Network Configuration Policy

- Hidalgo County Information Technology is responsible for the Hidalgo County network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent Hidalgo County network infrastructure capable of exploiting new networking developments, all cabling must be installed by Hidalgo County IT, IR system administrator or an approved contractor.
- All network connected equipment must be provided by and configured to a specification approved by Hidalgo County IT.
- All network equipment connected to Hidalgo County networks is subject to Hidalgo County IT management and monitoring standards. (with certain exceptions: Law enforcement)
- Changes to the configuration of active network management devices must not be made without the approval of the Hidalgo County IT Department.
- The Hidalgo County network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by Hidalgo County IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by Hidalgo County IT.
- All connections of the network infrastructure to external third party networks are the responsibility of Hidalgo County IT. This includes connections to external telephone networks.
- The use of departmental firewalls and other computer related security devices is not permitted without the written authorization from Hidalgo County IT.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Hidalgo County network without Hidalgo County IT approval.
- Users must not install network hardware or software that provides network services without Hidalgo County IT approval.
- Users are not permitted to alter network hardware in any way.

Policy 8.00 – Password Policy

- Passwords must be changed at least every 90 days.
- Passwords should contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#$%^&*_+=?/~`;:,<>|\).
- Passwords must not be easy to guess and they:
  - should not be your Username, must not be your employee number, must not be your name, must not be family member names, must not be your nickname, must not be your social security number, must not be your birthday, must not be your license plate number, must not be your pet's name, must not be your address, must not be your phone number, must not be the name of your town or city, must not be the name of your department, must not be street names, must not be makes or models of vehicles, must not be slang words, must not be obscenities, must not be technical terms, must not be school names, school mascot, or school slogans, must not be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.) ,must not be any popular acronyms, must not be words that appear in a dictionary, must not be the reverse of any of the above.
- Passwords must not be reused for a period of one year
- Passwords must not be shared with anyone
- Passwords must be treated as confidential information

Suggestions on creating a strong password:

- Combine short, unrelated words with numbers or special characters. For example: eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
  - livefish - is a bad password
  - L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
  - l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable.

Policy 9.00 – Physical Access Policy

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Resources restricted facilities must be documented and managed.
- All IR equipment, systems and facilities must be physically protected in proportion to the criticality or importance of their function at Hidalgo County.
- Access to Information Resources facilities must be granted only to Hidalgo County support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an Information Resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Requests for access must come from the applicable Hidalgo County data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Resources facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the Information Resources facility.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for Information Resources facilities must be kept for routine review by the IR system administrator, elected official or department head based upon the importance of the Information Resources being protected. The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals that change roles within Hidalgo County or are separated from their relationship with Hidalgo County.

- Visitors must be escorted in card access controlled areas of Information Resources facilities.
- The person responsible for the Information Resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the Information Resources facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Policy 10.00 – Information Technology Privacy Policy

- ALL Electronic media (analog and digital; video, audio, text messages blog entries, data files or other media) created, sent, received, recorded or otherwise stored on information resources owned, leased, administered, connected to or otherwise under the custody and control of Hidalgo County are not private and may be accessed by Hidalgo County at any time without knowledge of the IR user or owner.
- Electronic media controlled by Law Enforcement may, in certain cases, be deemed evidence and not subject to access by non law enforcement staff.
- To manage systems and enforce security, Hidalgo County may log, record, review, and otherwise utilize any information stored on or passing through its IR systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. For these same purposes, Hidalgo County may also capture user activity such as: emails, telephone numbers dialed, web sites visited, etc.
- A wide variety of third parties have entrusted their information to Hidalgo County for business purposes, and all workers at Hidalgo County must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.
- Users may not use county stored data for personal gain or individual profit.
- Users must report any weaknesses in Hidalgo County computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access or install any data or programs contained on Hidalgo County systems for which they do not have authorization or explicit consent from the department system administrator or the IT department.

Policy 11.00 – Security Training Policy

- IT policies are included in the County wide policy and procedure manuals.
- IT must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

Policy 12.00 – Software Licensing Policy

- Hidalgo County provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.
- Third party copyrighted information, software, audio and video files, that Hidalgo County does not have specific approval to store and/or use, must not be stored on Hidalgo County systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).
- Third party software in the possession of Hidalgo County must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.
- IR System administrators through the IT department will publish a list of authorized software that can be installed on PCs and will be supported. Any software not on this list must be installed only by specific permission from the IR System administrator.
- IT and the IR System administrator will reserve the right to remove any software that it deems unnecessary, therefore unsupported.

Policy 13.00 – Virus Protection

- All workstations whether connected to the Hidalgo County networks, or standalone, must use the Hidalgo County approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each file server attached to the Hidalgo County network must utilize Hidalgo County IT approved virus protection software and setup to detect and clean viruses that may infect file shares.
- E-mail gateway(s) must utilize Hidalgo County IT approved e-mail virus protection software and must adhere to the IT rules for the setup and use of this software.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IR system administrator and the IT Department.

Policy 14.00 – I.T. Staffing

- The I.T. Department is the only department that maintains and manages I.T. systems, equipment and infrastructure on a countywide level.
- All job titles that include the term “IT”, “computer”, “PC”, “telephone”, “network”, “GIS” or are of a computer related nature are for the exclusive use of the IT Department.
- All PC repair technician positions MUST report directly to the CIO and be part of the County’s IT Departments Technician repair pool.
- The title IT Manager must be exclusively used for the IT Department.
- All IT Department staff is bound by confidentiality agreements signed upon entry into the department.