

Data Security Policy

Table of Contents

Data Security Policy.....	1
Overview	1
Security Objectives	1
Working with Independent Service Providers	2
Threats to Security Controls	2
Theft of Information.....	2
Malicious Destruction of Data	4
Unauthorized Financial Transactions	4
Passwords and User ID Integrity	5
Catastrophic Events.....	6
Reporting Attempted or Actual Breaches of Security	7
Review and Revisions Policy.....	7
Appendix A – Recommended Software Packages.....	7
A1 Encryption Packages	7
A2 Security Erase Packages.....	8
A3 Password Management Packages.....	8
A4 Specifically Prohibited Software	9
Appendix B – Policies Included in this Policy by Reference	10

Overview

The Hillsdale Housing Commission’s data is a valuable asset. People trust the Hillsdale Housing Commission to keep information confidential. The Hillsdale Housing Commission is required to have policies and procedures that protect against accidental or intentional misuse of the information used by the Hillsdale Housing Commission.

The Hillsdale Housing Commission is committed to preserving and protecting Commission information. To that end, the Hillsdale Housing Commission has developed and adopted this Data Security Policy.

Security Objectives

The Information Security Program at Hillsdale Housing Commission is designed to ensure that the following security objectives are met:

1. Commission data and records will be kept secure and confidential. The Commission shall implement and maintain a series of controls that help safeguard information from access by persons not authorized by the Executive Director and/or the Hillsdale Housing

Commission board. Data will not be sold, exchanged, or given away without the prior written consent of the Executive Director and/or the Hillsdale Housing Commission.

2. Known and anticipated threats to the Hillsdale Housing Commission's Security Program will be documented, along with measures taken to minimize the likelihood of such threats reoccurring.
3. The Executive Director will be proactive in searching for new threats to the Commission's Security Program. Specifically, the Executive Director will attend seminars, training classes, and read pertinent literature on how to protect Commission information. The Housing Commission will also conduct periodic reviews of its information technology security operations.

Working with Independent Service Providers

The Hillsdale Housing Commission will periodically work with Independent Service Providers. Most notably, the Commission will contract with third parties to perform property management, financial and other types of audits, and management reviews. The Commission may also purchase data processing services from various organizations, send checks, wire transfers and Commission transactions to affiliated and non-affiliated banks, and transmit and receive data from credit bureaus.

In all instances, unless the Independent Service Provider is a government entity covered under the *Freedom of Information Act*, (5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048), the Commission will require a written statement from the Service Provider wherein the Provider attests to having a Security Program that meets the security objectives outlined in this policy. If the Service Provider refuses to provide such a statement, the service contract will be abrogated.

(Note: contracts currently in force are excluded from this requirement, unless the contract expires subsequent to July 1, 2003. Contract expiring subsequent to this date will be amended to stipulate that suitable security procedures will be maintained.)

Threats to Security Controls

This portion of the policy identifies potential threats to Hillsdale Housing Commission's Security Controls, and what the Commission has done to address them.

Theft of Information

The theft of confidential information could result in the Hillsdale Housing Commission's residents, applicants, clients, Commissioners and employees being victims of identify theft. This section is intended to address the Commission's steps to avoid theft of information.

1. All discarded reports and other confidential information shall be securely stored until it can be shredded or otherwise destroyed.
2. All Commission reports and documents shall be secured prior to leaving for the day.

3. Authorized users may electronically transmit data necessary for normal Commission activities to contracted third parties (including accountants, auditors and property management software contractors) with a need to know via e-mail, Secure Socket Layer (SSL) transmission or other secure method, under the following conditions:
 - a. The Executive Director shall maintain a list users authorized to transmit data and of authorized agencies to which the data may be transmitted. Deliberate data transmission to unauthorized agencies may result in disciplinary action or termination.
 - b. Confidential data sent via e-mail or any non-secure electronic transmission method shall be encrypted prior to transmission. A copy of the encrypted file shall be maintained on the Commission's network, along with a record of transmission. The Executive Director shall be responsible for maintaining a list of data which shall be transmitted in an encrypted manner, and all authorized users shall be responsible for requesting this information prior to transmitting the data.
 - c. Acceptable encryption techniques include password-protected .Zip files as well as use of other encrypting software.
 - i. The Executive Director shall be responsible for negotiating an acceptable method of encryption with the contractor to whom data is being transmitted, to ensure that the encryption method is acceptable to both parties.
 - ii. Wherever possible, "strong" encryption techniques shall be used for transmission. When the vendor is unable to use "strong" encryption techniques, "weak" encryption shall be deemed acceptable. However, the contractor shall be encouraged to participate in a data integrity program which includes "strong" encryption. (See Appendix A for a sample list of encryption software packages.)
4. Computer hard drives and erasable electronic media (such as floppy disks, archival tapes, external hard drives, etc.) removed from service shall be completely erased and security wiped prior to disposal. The Commission shall use a software package that meets government security standards to erase electronic media (See Appendix A for a sample list of security erase software packages), and staff shall follow instructions included with the utility to assure data destruction.
5. For computer media removed from service that may not be erased (i.e., recordable CD-ROMs or DVD-ROMs), the media itself shall be thoroughly destroyed so as to render data unsalvageable.
6. Portable computers (including laptops, notebook PC's, tablet and slate PC's and PDAs) shall be secured to avoid theft and/or unauthorized system access whether on or off of Commission property.
 - a. Users of such portable computers shall know the whereabouts of the computers at all times. Users of such portable computers shall immediately report any loss or theft to the Executive Director.

- b. The Hillsdale Housing Commission shall require users of portable computers to employ the use of hardware, software, biometric, BIOS passwords or other security mechanisms to ensure that data from a lost or stolen portable computer is not accessible to any person who may find the computer. The Executive Director shall be granted access to all systems with administrative rights.
 - c. The Hillsdale Housing Commission may require that users of portable computers employ the use of stealth tracking software designed to locate the machine in case of loss or theft. The Hillsdale Housing Commission may also employ the use of software that renders data contained in the portable computer inaccessible in case of loss or theft. Because such software may interfere with the normal operation of the computers, the Executive Director shall determine whether such measures are necessary on a case-by-case basis.
7. Malware, including adware, spyware, or other malicious software shall not be installed on any Commission PC at any time. The Executive Director shall maintain a list of approved programs which may be installed on each PC and shall ensure that approved programs do not appear as malware on such sites as www.spychecker.com. (See Appendix A for a list of specifically prohibited software.)

Malicious Destruction of Data

The purposeful destruction of customer data could result in the Hillsdale Housing Commission being unable to process charges, payments or correctly calculate rent, among other difficulties. This section is intended to address the Commission's steps to avoid malicious destruction of data.

1. To protect against viruses and other types of attacks, the Hillsdale Housing Commission shall install and maintain current versions of virus protection software, as described in the Commission's *Acceptable Computer Use Policy*.
2. The Hillsdale Housing Commission will purchase and install either:
 - a. A hardware firewall device for the entire network, or,
 - b. A software firewall package for each machine which connects to the network or the Internet.
3. Commission employees shall check each month for updates for the firewall software or firmware, and all updates shall be installed when the update is determined to be stable.

Unauthorized Financial Transactions

The Hillsdale Housing Commission could suffer a material loss in the event an employee embezzles, misappropriates, or otherwise misuses funds by making withdrawals from Commission accounts. This section is intended to address the Commission's steps to avoid unauthorized financial transactions.

1. Security systems incorporated into primary financial systems shall be used to enforce a reasonable separation of duties.
2. All on-line financial transactions shall be reviewed and approved by the Executive Director.
3. The ability to change name and address information on financial transactions is exclusively limited to the Executive Director, and the Hillsdale Housing Commission shall review all such transactions.
4. The Executive Director shall review newly entered financial transactions on a regular basis (at least once per calendar month).
5. The Hillsdale Housing Commission shall use anti-fraud measures for all issued checks, including, but not limited to, watermarked checks, requiring check endorsement signatures and/or stamps, and adherence to bank or financial institution methods of identification, such as thumb/fingerprints or photo identification.
6. The Executive Director or his or her designee shall conduct reconciliation of all transactions on a periodic basis (at least monthly).
7. Employees and Commissioners shall adhere to the Commission's *Credit Card Policy*, hereby incorporated into this Policy by reference.
8. Employees and Commissioners shall adhere to the Commission's *Funds Transfer Policy*, *Procurement Policy*, *Check Signing Authorization Policy*, *Ethics Policies*, and other existing Commission policies to ensure the integrity of financial transactions. The Commission's *Funds Transfer Policy*, *Procurement Policy*, *Check Signing Authorization Policy* and *Ethics Policy* are hereby included as a portion of this Policy by reference.

Passwords and User ID Integrity

An unauthorized individual could post invalid transactions, misuse tenant information, or disrupt service by using an unauthorized user-ID and/or password. This section is designed to enforce password and user ID integrity.

1. All authorized Commission staff shall be assigned individual user IDs and passwords for internal Commission systems and external HUD and other systems. The Executive Director shall maintain a list of authorized users and the level of access allowed for each system shall be likewise documented.
2. Commission staff shall regularly change passwords to all systems and inform the Executive Director of the change. The following methods shall be observed regarding passwords:
 - a. Passwords shall not be comprised of simple names and/or dates.
 - b. Passwords will be comprised of random letters and numbers and shall be at least six (6) characters in length.

- c. Employees shall not use the same password for different accounts, and shall use different passwords each time a password is changed. Users shall not use the same password more than once.
 - d. Passwords shall not be written down, printed out, posted in areas accessible to others, or otherwise made available for others to access.
 - e. Users are encouraged to use a password management software package to manage stored passwords. (See Appendix A for a sample list of password management software packages.).
 - i. Password management software packages shall ensure that all passwords are maintained within a master encrypted file.
 - ii. Users shall not share the master password for any password management software package. Since federal regulations prohibit sharing HUD and other governmental passwords, the user shall not divulge the password to the Executive Director, Hillsdale Housing Commission, or any other individual or agency.
 - f. The Executive Director shall be immediately notified of any change of user names or passwords for any system which locks the user out of the system previously granted access.
3. All Commission staff shall be made aware of the risk of termination for sharing user IDs or passwords. Such risk shall include, but not be limited to, disciplinary measures, termination or restriction of user access to accounts, termination of employment, civil and criminal charges.
 4. Terminated users User IDs and Passwords shall be immediately removed from all systems. The Executive Director shall be responsible for ensuring that terminated user IDs and passwords are removed from systems in a timely manner.

Catastrophic Events

The destruction of Hillsdale Housing Commission data as a result of fire, tornado or other catastrophic event could result in a loss of customer records, and vital agency data. This section is designed to help prevent against data loss as a result of catastrophic events.

1. All computer files shall be backed-up on a periodic basis, the frequency of which shall be determined and based on need by the Executive Director, but shall be no less than once per calendar week of operation. The backup media shall be compared to the original to ensure data integrity. The Executive Director shall ensure that staff are trained in backup and security procedures contained in this Policy and the *Acceptable Computer Use Policy*.
2. The backup files shall be stored on removable media at a separate location from the original data.
 - a. Acceptable storage shall include off-site storage or in a fireproof container in the Commission's offices.

- b. If an off-site storage location is selected, it shall be located far enough from the main data location to minimize the risk that one catastrophe will destroy both the primary and backup data files. Commission staff shall ensure that the backup media is secured from theft and other catastrophes at the off-site storage location.
 - c. If storage of backup media in a fireproof container in the Commission's offices is selected, staff shall ensure that the backup media is secured immediately following completion of the backup.
3. Staff shall not use on-line backup services for backup purposes, since the Commission has no control over the data once it leaves the Commission's network.

Reporting Attempted or Actual Breaches of Security

All breaches and attempted breaches of the Commission's security controls will be referred to the appropriate legal authorities. All breaches and attempted breaches will also be reported to the Executive Director and the Executive Director shall report same to the Housing Commission board.

Review and Revisions Policy

The Executive Director is responsible for maintaining this Policy and ensuring compliance. This Policy will be reviewed and revised by Commission resolution, as needed.

Appendix A – Recommended Software Packages

A1 Encryption Packages

The following is a list of data encryption software packages that are representative of the encryption needs of the Hillsdale Housing Commission. This list is not meant to be inclusive; it is provided as a guide to help the Policy administrator locate and evaluate software packages which may suit the Commission's needs. Products are listed below in no order of preference.

(Note: as of the date of adoption of this policy, Blowfish, AES, and other software encryption [included in PGP and other encryption packages] are considered "strong" encryption algorithms. Password-protected .Zip files are considered to be "weak" encryption algorithm. This Section should be changed as software developers implement or change encryption methods.)

Name	Vendor	Description	URL
3eee Triple Encryption Small Client	3eee	Freeware – From the developer: 3eee Triple Encryption will encrypt any disk file quickly, reliably and with strong encryption algorithms. Simply use the easy 3eee Console to select and encrypt/decrypt files or right click a file and select encrypt	www.3eee.com
k-Crypt Encryption	k-Crypt	Freeware – From the developer: k-Crypt is a powerful encryption tool that uses AES encryption techniques. It is a 'must-have' for anyone who wants to safeguard his	www.k-crypt.net/

		<i>data. k-Crypt is overall, a neat, user-friendly and powerful encryption tool. U.S. Government organizations (and others) to protect sensitive information.</i>	
Pretty Good Privacy	PGP	Free for Noncommercial Use – From the developer: <i>PGPfreeware builds on the heritage of PGP, which was originally released as freeware and today has millions of users worldwide. Features include PGPtray, a Clipboard encryption system that is accessible from the system tray; seamless integration with Qualcomm's Eudora e-mail plug-in for Microsoft Outlook/Exchange; a Windows Explorer context menu for direct access to all PGP functions; secure file wiping; and recipient groups for easy encryption to multiple recipients.</i>	http://www.pgp.com/

A2 Security Erase Packages

The following is a list of security erase software packages that are representative of the security erasure needs of the Hillsdale Housing Commission. This list is not meant to be inclusive; it is provided as a guide to help the Policy administrator locate and evaluate software packages which may suit the Commission's needs. Products are listed below in no order of preference.

Name	Vendor	Description	URL
Wipe Info	Symantec	Commercial product – included in the Norton Utilities and Norton SystemWorks suite.	www.symantec.com
Eraser	Heidi Computers	Freeware – From the developer: <i>Eraser is an advanced security tool (for Windows), which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.</i> <i>Eraser is FREE software and its source code is released under GNU General Public License.</i>	http://www.heidi.ie/eraser/
QuickWiper	AKS Labs	Freeware – From the developer: <i>Utility which lets you wipe files. "Wipe" means deleting file so they could never be undeleted or recovered. QuickWiper lets clear your cookies records, IE history, cache, typed URLs and links to recently opened files. Wiping free space with QuickWiper allows to you wipe all previously deleted files.</i>	http://www.aks-labs.com/

A3 Password Management Packages

The following is a list of password management software packages that are representative of the password management needs of the Hillsdale Housing Commission. This list is not meant to be inclusive; it is provided as a guide to help the Policy administrator locate

and evaluate software packages which may suit the Commission’s needs. Products are listed below in no order of preference.

Name	Vendor	Description	URL
Password Pro 32	ZDNet	Freeware – blowfish encryption, random password generation.	www.zdnet.com/downloads
ABI- Key/Password Manager	ABI Software Development	Shareware – From the developer: <i>ABI- Key/Password Manager is designed to keep track and manage your passwords and keys while protecting them from unauthorized access. It secures your keys and passwords by using a 448 bit Blowfish encryption algorithm, also used in our encryption software ABI- CODER and ABI- SecurePro.</i>	www.abisoft.net
Password Agent Lite	Moon Software	Freeware – From the developer: <i>Password Agent is a password manager program that allows you to store all your passwords, secret notes and data snippets in a single, easy to navigate, and secure database. Too many passwords to remember? Pieces of paper that you once used to write down your important account information are lost? Want to find required password quickly? Password Agent keeps track all of your different passwords - no problems, no worries. And, it keeps strangers away from accessing your private information.</i>	www.moonsoftware.com/

A4 Specifically Prohibited Software

The following is a list of software packages that are specifically prohibited from installation on Hillsdale Housing Commission computers. This list is not meant to be inclusive; it is provided as a guide to help the Policy administrator determine which software packages may result in theft of data and/or data loss. Products are listed below in no order of preference.

DoubleClick	Yo Mama	Osama (game)
Aureate Media	Hotbar	Comet Cursor,
Conducent Timesink	Cydoor	Flashpoint/Flashtrack
Gator/Gator eWallet	GoHip	Mattel Broadcast
SongSpy	Web3000	WebHancer
RadLight	Morpheus	Kaaza

AudioGalaxy	WinMX	Grokster
-------------	-------	----------

Appendix B – Policies Included in this Policy by Reference

- Hillsdale Housing Commission *Acceptable Computer Use Policy*
- Hillsdale Housing Commission *Credit Card Policy*
- Hillsdale Housing Commission *Funds Transfer Policy*
- Hillsdale Housing Commission *Check Signing Authorization Policy*
- Hillsdale Housing Commission *Ethics Policy*

Adopted by the Hillsdale Housing Commission on: (date), Resolution # (Res. No.)

DRAFT