HillSouth
Security Policy Manual

Revision History

Version	Date	Author	Summary of Changes
1.0	00/00/00		Orig
2.0	12/01/19	Valazure	Signature page added, reviewed.

Approvals

Table of Contents

1.0 Introduction

Control Number:

Control Objective:

Item Name:

Task:

HillSouth's network is an important resource for achieving our business objectives. Critical resources, such as databases, patient information, client data, and private employee information are areas that must be protected from intrusion and inappropriate use or disclosure. Systems themselves must be set up and routinely updated so they prevent intrusion and other malicious activities.

The purpose of this policy is to ensure that all individuals utilizing HillSouth's resources understand their responsibility in reducing the risk of compromise and take appropriate security measures to protect our company's systems and data. Everyone at HillSouth has a responsibility to assist with the implementation and enforcement of this policy.

HillSouth will use the appropriate personnel, vendor or affiliate policies to adjudicate violations such as failure to comply with this policy, not taking corrective action when notified, system or network misuse or improper disclosure of protected information.

2.0 Acceptable Use Policy

Control Number:

Control Objective:

Item Name:

Task:

2.1 Overview

HillSouth's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to HillSouth's established culture of openness, trust and integrity. HillSouth is committed to protecting our employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of HillSouth. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every HillSouth employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. Security procedures are sought from many external sources on an ongoing basis to stay current with new technologies and systems.

2.2 Purpose

This policy outlines the acceptable use of computer equipment at HillSouth for the purpose of protecting HillSouth, HillSouth's employees, clients, and partners. Inappropriate use exposes HillSouth to risks including virus attacks, compromise of network systems and services, and legal issues.

2.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at HillSouth, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by HillSouth.

2.4 Policy

2.4.1 General Use and Ownership

1. All data that users create on the corporate systems remains the property of HillSouth. Management does not guarantee the confidentiality of personal information stored on any network device belonging to HillSouth.
2. Employees should exercise good judgment regarding the personal use of company assets. In the absence of such policies, employees should be guided by departmental policies on personal use. For questions regarding acceptable usage, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within HillSouth may monitor equipment, systems and network traffic at any time.

4. HillSouth reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4.2 Security and Proprietary Information

1. The information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the Information Sensitivity policy. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords must be changed at least every 42 days for domain accounts and 90 days for Connections accounts.
3. All users are required to lock the screen (control-alt-delete for Win2K/XP users) of their PC, laptop, or workstation when it will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a HillSouth email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of HillSouth, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the HillSouth Internet/Intranet/Extranet, whether owned by the employee or HillSouth, shall be continually executing approved virus-scanning software (Symantec Corporate Antivirus Protection) with current virus definitions.
7. Employees should avoid or must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Trojans, or other forms of malware.

2.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of HillSouth authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing HillSouth-owned resources.

The list items below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of

"pirated" or other software products that are not appropriately licensed for use by HillSouth.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which HillSouth or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, etc.).
5. Revealing account passwords to others or allowing others usage of an account not their own. This includes family and other household members when work is being done at home.
6. Using a HillSouth computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any HillSouth account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to HillSouth is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, HillSouth employees to parties outside HillSouth unless it is a part of normal job duties.

2.5 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within HillSouth's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by HillSouth or connected via HillSouth's network.
7. Posting the same or similar non-business-related messages to large numbers of email recipients (spam).

2.6 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.7 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

3.0 Access Control Policy

Control Number:

Control Objective:

Item Name:

Task:

HillSouth has established the following policy to define how access control to information systems and services cover all stages in the life cycle of user access: from registration of new users to de-registration of users who no longer need access. Where possible, user policies are enforced by the operating system or other software.

- HillSouth data must have sufficient granularity to allow appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. HillSouth recognizes this balance.
- Where possible and financially feasible, more than one person must have full rights to any HillSouth owned server storing or transmitting highly sensitive data. HillSouth has a standard policy that applies to user access rights.
- Access to HillSouth's network, servers and systems is achieved by individual and unique logins, and requires authentication. Authentication may include the use of passwords, smart cards, biometrics, and/or other recognized forms of authentication.
- As stated in HillSouth's policy on appropriate and acceptable use, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system access from unauthorized use.
- All users of HillSouth systems that contain high risk or confidential data must have a strong password - the definition of which is established in HillSouth's password policy. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established in the password policy.
- Default passwords on all HillSouth systems are changed after installation. All administrator or root accounts are given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords are not coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all HillSouth authentication devices. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access is reviewed and adjusted as found necessary. Terminated employees have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews are conducted by the Network Administrator.
- Transferred employee access is reviewed and adjusted as found necessary.
- Physical access to HillSouth is controlled using individual proximity key card. HillSouth has ten access levels.

- Monitoring has been implemented on all HillSouth systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
- Activities performed as administrator are logged where it is feasible to do so.
- Personnel who have administrative system access use other less powerful accounts for performing non-administrative tasks.

4.0 Physical Security Policy

Control Number:

Control Objective:

Item Name:

Task:

4.1 Purpose

The purpose of the HillSouth Physical Security Policy is to establish the rules of granting, controlling, monitoring, and removing physical access to HillSouth's facilities, property and equipment.

4.2 Scope

The Physical Security Policy applies to all individuals that have been granted access to HillSouth's facilities, property and equipment.

4.3 Policy

HillSouth resources must be physically protected in proportion to the criticality, sensitivity, or business importance of their function(s).

- All physical security systems must comply with all applicable regulations, including, but not limited to, building codes and fire prevention codes.
- Restricted areas and facilities must be clearly marked. Signage for restricted areas and facilities should contain enough information to be practical, but present minimal discernible evidence as to the nature of the importance of the location.
- Each individual granted physical access to restricted Information Resources or facilities must receive training on emergency procedures for the facility.

4.3.1 Surveillance

- Physical access to all restricted Information Resources and facilities must be documented.
- All facilities that allow visitors must track visitor access with a sign in/sign out log.
- Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- The Security Administrator must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- HillSouth employs video surveillance technology to deter theft, violence and other criminal activity.
  - In the event of a reported or observed incident, the recorded footage may be used to assist in the investigation of the incident and may be turned over to law enforcement personnel, if appropriate.
  - At no time will persons other than those designated have access to the footage made in the course of surveillance. Personal

information contained on the footage shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

  - Footage from the surveillance cameras will be kept until the database reaches its storage limits; the oldest data will be purged first unless required for the purposes outlined in this policy. If footage has been used to investigate an incident, that footage will be retained for one year after a final decision is reached concerning the incident.
  - Old footage that isn't reused or recycled for surveillance will be shredded, burned, or otherwise made permanently unreadable.

4.3.2 Security Access System

- Personnel, including full- and part-time staff, contractors, and vendor service staff, should be granted access only to facilities and systems necessary to fulfill their job responsibilities.
- Requests for access must come from and include sign-off from an applicable data/system owner.
- The process for granting physical access to Information Resources facilities must include the approval of the Security Administrator.
- Each individual granted physical access to an Information Resources facility must sign appropriate access, information protection, and nondisclosure agreements.
- The Help Desk must remove card and/or key access rights of individuals that leave or change roles within HillSouth.
- The Help Desk reviews card and/or key access rights for the facility on a quarterly basis as a part of the Security Access Audit and remove access for individuals that no longer require access.
- Visitors who have not been granted special access privileges must at all times be escorted and monitored in access-controlled areas at HillSouth facilities.

4.3.3 Protection of physical access cards and keys

- Personnel must not share or transfer access cards and/or to other individuals within or external to HillSouth including "piggybacking" i.e. allowing fellow employees or other individuals to follow into an access controlled area without appropriate permissions.
- Access cards and/or keys that are no longer needed must be returned to the Help Desk. Cards must not be transferred or reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the Help Desk.
- A service charge may be assessed for access cards and/or keys that are lost, stolen, or not returned.

4.4 Enforcement

Gross negligence or willful disregard of this standard may result in disciplinary action which may include loss of HillSouth access privileges, termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals may be subject to civil and criminal prosecution.

5.0 Anti-Virus Software Policy

Control Number:

Control Objective:

Item Name:

Task:

- All workstations and servers owned and operated by HillSouth are required to run the Symantec Corporate Antivirus software.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying the computer's Recycle Bin.
- Delete spam, chain, and other junk email without forwarding, as per HillSouth's Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan removable disks from an unknown source for viruses before using them.
- If testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Virus definitions are automatically updated daily by Symantec Corporate Antivirus.

6.0 Automatically Forwarded Email Policy

Control Number:

Control Objective:

Item Name:

Task:

6.1 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

6.2 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of HillSouth.

6.3 Policy

Employees must exercise utmost caution when sending any email from inside HillSouth to an outside network. Unless approved by an employee's manager, HillSouth's email will not be automatically forwarded to an external destination. Sensitive information, as defined in the Information Sensitivity Policy, will not be forwarded via any means, unless that email is critical to business.

6.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.5 Definitions

Terms	Definitions
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to HillSouth or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

7.0 Backup / Restore Policy

Control Number:

Control Objective:

Item Name:

Task:

7.1 Overview

This policy defines the backup policy for computers within HillSouth which have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers backed up include file, mail, database, application, and web.

7.2 Purpose

This policy is designed to protect data within HillSouth to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

7.3 Scope

This policy applies to all equipment and data owned and operated by HillSouth, Inc.

7.4 Definitions

Term	Definition
Backup	The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
Archive	The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
Restore	The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

7.5 Timing

Incremental backups are performed nightly on Sunday, Monday, Tuesday, Wednesday, Friday and Saturday. If for maintenance reasons, backups are not performed on Saturday, they are rescheduled for Sunday. Full backups are performed every Thursday. If for any reason a full backup fails, it is rescheduled for either Friday or Sunday.

Full data replication of scanned patient files, including prescriptions and reports, and scanned billing documentation and invoices is done real time using our SANs data replication technology. HillSouth also utilizes Oracle's DataGuard technology to replicate production data to both onsite reporting and offsite disaster recovery standby databases. As data is changed on the production systems, that data is shipped via Oracle DataGuard to both standby databases. This is done approximately every 2 hours throughout the day. In case of primary database failure, the standby database can be configured as the primary database with minimal configuration changes. The use of

Oracle DataGuard and standby databases reduces downtime due to primary database failure and provides for business continuity in case of a catastrophic event.

7.6 Backup Media

HillSouth does not utilize tape backup. All backup is done disk to disk over our 45 Mbps point to point DS3 to an offsite storage location (See 6.11). All back up sets are encrypted using an AES 128bit encryption key.

7.7 Responsibility

Backup success and failure reports are emailed to Production-Alarms and the System Administrator. All failures are monitored by the System Administrator and the IT management team. Errors are corrected and a manual backup is run upon backup failure.

7.8 Testing

The ability to restore data from backups shall be tested at least once per month using actual test restores.

7.9 Data Backed Up

Data to be backed up include the following information:

1. Patient documents
2. Billing invoices
3. Production Connections ™ database
4. Production Oracle Financials database
5. User data stored on the file servers
6. Active Directory user and computer data
7. Exchange information stores
8. Subversion Repositories

Systems to be backed up include but are not limited to:

1. File servers
2. Mail servers
3. Domain controllers
4. Production database servers
5. Test database server
6. Versioning control server

7.10 Restoration

Users that need files restored must submit a change request to the IT Infrastructure department. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

7.11 Offsite Storage Locations

Offsite storage is warehoused at our collocation facility, Peak10. Peak10's data centers include redundant HVAC system keep the average temperature in each data center at 70 degrees Fahrenheit. Peak 10 data centers utilize dry-fire suppression systems that can be deployed manually, or by a sequence of three failures anywhere in a data center zone. Peak10 utilizes a 5 level security system maintain security to their data centers.

7.12 Backup Software

HillSouth currently uses Symantec Backup Exec 12d software to perform disk to disk backups. Real time replication is performed using either CA XOSoft High Availability software or our Compellent SANs data replication features. Database replication is performed using Oracle DataGuard.

7.13 Documentation Review

HillSouth's Network Administrator ensures that backup documentation is kept current by performing a quarterly review of documentation or designating a staff member to perform a review. The Test Track requests within the last quarter should be reviewed to help determine whether any changes were made. Also any current or completed projects affecting data storage should be reviewed to determine whether there were any changes made to support the project.

8.0 Operational and Software Development Change Management Policy

Control Number:

Control Objective:

Item Name:

Task:

8.1 Policy

This policy describes the responsibilities, policies, and procedures to be followed when making changes or recording events to the HillSouth IT infrastructure and applications.

8.2 Mission Statement

The System Administrator, Internal Help Desk, EDI and Applications teams are tasked with providing a stable and reliable IT infrastructure and applications for HillSouth. The purpose of this Change Management process is to minimize service disruptions to our computing environment and promote system availability.

8.3 Policy/Procedure Maintenance Responsibility

The System Administrator, Internal Help Desk, EDI and Applications teams are responsible for maintaining and updating this Change Management Policy/Procedure.

8.4 Definitions

Term	Definition
Change	To transform, alter, or modify the operating environment or standard operating procedures; any modification that could have a potential and/or significant impact on the stability and reliability of the infrastructure and impacts conducting normal business operation; any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.
Event	Any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period. *Change and Event will be used interchangeably throughout this document.*
Change Request	The official notification of the change/event submitted using Test Track.

8.5 Purpose

The Change Management Process is designed to provide an orderly method in which changes to the IT environment are requested and approved prior to the installation or implementation. The purpose is not to question the rationale of a change, but to ensure that all elements are in place, all parties are notified in advance, and the schedule for implementation is coordinated with all other activities within the organization.

8.6 Scope

Change Management provides a process to apply changes, upgrades, or modifications to the IT environment. This covers any and all changes to the hardware, software or applications. This process also includes modifications, additions or changes to the LAN/WAN, Network or Server hardware and software, and any other environmental shutdowns (electrical). The process is for any change that might affect one or all of the environments HillSouth relies on to conduct normal business operations. It also includes any event that may alter the normal operating procedures.

Changes to the IT environment arise from many circumstances, such as:

- Periodic maintenance
- User requests
- Hardware and/or software upgrades
- Acquisition of new hardware and/or software
- Changes or modifications to the infrastructure
- Environmental changes
- Operations schedule changes
- Changes in hours of availability
- Unforeseen events

The above list is not all-inclusive. If you are unsure if a change needs to be submitted through the Change Management process, you should contact the Internal Help Desk.

8.7 Submission of a Change Request

The requester must submit a change request.

All change requests shall be submitted using Test Track.

The change request must include enough detail so that all areas know the relative impact of the change and how it may affect other areas.

The Test Track change request form shall be submitted directly through the web interface. If you do not know how to complete the Test Track request form or you do not know how to access the website, you may contact the Internal Help Desk.

If a change is submitted and is in conflict with a previous change request, the change will not be posted and the Internal Help Desk will notify the parties of the conflict. The first requested change will remain posted until the parties notify the Internal Help Desk of the resolution, preferably by email.

If the parties cannot reach an agreement, the issue shall be elevated to the CIO for resolution, and again the resolution is to be submitted to the Internal Help Desk.

8.8 Updating, Correcting, or Withdrawing a Change Request

Once a Change Request has been submitted and a situation arises that the request must be updated, corrected, or withdrawn, an email is to be sent to the Internal Help Desk ASAP requesting the change submission be deleted. A new Test Track change request form must be submitted to the Internal Help Desk for updates or corrections. An exception to this requirement may be a minor correction in the content of the previously submitted request. If there is a question as to whether or not a new form should be submitted, please contact the Internal Help Desk.

8.9 Emergencies

Emergencies exist only as a result of:

- a user's computer is completely out of service
- there is a severe degradation of service needing immediate action
- there is an outage in communication with customers or vendors
- a system/application/component is inoperable and the failure causes a negative impact
- a response to a natural disaster
- a response to an emergency business need

All emergencies are handled on an as-required basis with the approval of the System Administrator & Internal Help Desk and must follow the guidelines below:

Send an email or otherwise call the Internal Help Desk either before or immediately after the change/event occurs.

The emergency email should include at a minimum the following information:

- what additional users have been affected and who needs to be notified
- external user names and or phone number, when applicable
- if there is a possible work around until the problem is resolved
- approximate time event or change occurred
- the approximate length of the outage
- notification of resolution, if any
- any error messages or alerts if applicable

Emergencies after normal business hours, on the weekend or holidays, will be resolved immediately and reported to the System Administrator (if network related). A completed Test Track change request form must be submitted through the regular reporting process on the first work day immediately following when the change was made or the event occurred.

The System Administrator & Internal Help Desk will review all emergency submissions to ensure the change met the criteria for an "emergency change" and to prevent the process from becoming normal practice to circumvent the Change Management Process.

8.10 Responsibilities

8.10.1 System Administrator & Internal Help Desk

The System Administrator & Internal Help Desk will direct the Change Management Process.

The System Administrator & Internal Help Desk responsibilities include the following tasks:

- Analyze and evaluate a Test Track change request as it relates to the impact on the HillSouth infrastructure.
- Approve or deny the change schedule in accordance with the HillSouth Change Management Policy, and report any deviations.
- Coordinate the changes/events.

- Notify parties of conflicts needing resolution.
- Send out notifications of any emergency changes or events.

8.10.2 Change Requester

It is the primary responsibility of the individual submitting a request to evaluate the change prior to submission.

The Change Requester's responsibilities include the following tasks:

- Evaluate the impact to the client, customer or vendor
- Document any error messages or alerts
- Document any important contact information (user/customer or vendors name, telephone number, extension or email address)
- Submit a complete, concise, and descriptive Test Track change request form.

Change Request Forms not completed properly will be rejected and returned to the Requester with an explanation for denial.

Once the request is approved the Internal Help Desk will perform the following tasks:

- Ensure that clients are aware of any possible impact.
- Coordinate proper on-site or on-call support as needed to resolve any problems or answer any questions that may occur during installation, or immediately subsequent to installation.
- Contact names and numbers should be available to support staff to obtain additional or outside support.
- Report unplanned outages or problems immediately.
- Provide a status update in the "Notes" section of the Test Track change request form upon completion of the requested change. The completed form must provide an update on the success or failure of the change in detail.

8.11 Unplanned Outages

All unplanned outages shall be reported to the System Administrator immediately. For any major outages, an outage notification report will be available within 24 hours of the resolved outage. The outage notification report will include such information as the type of outage, down time, clients affected, and resolution. All HillSouth employees are encouraged to provide accurate details of the problem and resolution. Cooperation and participation is required from all levels of management and staff to facilitate generating this report.

8.12 Test Track Prioritization

Following are examples of priorities for Change Management. This list is not all-inclusive. If you have doubts on whether your change should be requested through the Change Management process, contact the Internal Help Desk.

8.12.1 Severity

8.12.1.1 Cosmetic

Issues regarding the appearance or minor functionality glitches of the application that have little impact to the users being able to perform their jobs.

8.12.1.2 Workaround

Issues where users are still able to perform an activity via other means, but are not able use an application as it was intended.

8.12.1.3 No Workaround

Issues where users are not able to perform an activity by any means.

8.12.1.4 Causes Crash

Issue causes a crash for an application, server or system.

8.12.2 Priority

8.12.2.1 Urgent/Emergency

The problem requires immediate attention where either system failure or mission essential requirements are not available and no work around exists. This problem can apply to the system as a whole or to a user if system access is lost. The corrective action is implemented as soon as the fix is available regardless of change management schedule.

8.12.2.2 High

The problem is of high importance and can justify an out-of-cycle change. This priority is used for problems that meet Urgent requirements, except that a work around exists, or performance degradation for which no temporary work-around is available however delay would not cause adverse mission impact beyond that of inconvenience. These changes must still be controlled, tested and approved prior to implementation on a production system.

8.12.2.3 Medium

Routine Change Requests are judged less operationally important than High Priority and is not critical for implementation. This priority may be used for important software/hardware/network maintenance issues such as version upgrades, utility software, etc. This priority may be used to improve very difficult or awkward implementations for heavily used subsystems on a selective basis. This priority may be used for development activity or new requirements providing that the activity cannot be accomplished with the lower priority. These problems are resolved and implemented in the next scheduled change cycle.

8.12.2.4 Low

This priority is intended primarily for fixing capabilities that are currently operational but are difficult or awkward to use. It applies also to non-standard implementations, and other assorted irritants.

8.12.2.5 Future Release

This priority is intended primarily for gathering new requirements regarding unscheduled projects.

8.13 Types of Changes

Following are examples of candidates for Change Management. This list is not all-inclusive. If you have doubts on whether your change should be requested through the Change Management process, contact the Internal Help Desk.

8.13.1 Applications and Information Systems

Implementation of new applications, volume changes, new systems, new releases, or modifications. Migration from test to production of source code.

8.13.2 Backups and restores

Restoring data from backups, or performing special backups. If it is a restore, the reason for the restore must be provided, i.e. what happened to the original data.

8.13.3 Computing Systems Hardware

Hardware changes, additions, deletions, re-configurations, re-locations, preventive, or emergency maintenance.

8.13.4 Computing Systems Software

Program or OS hotfixes, product releases, versions, I/O and Network Control Programs (NCP), table changes, tuning, alterations to libraries, catalogs, monitors, traps, or changes to priority mechanisms, job classes, print classes.

8.13.5 Environmental

Power, UPS systems, generators, electrical work, facility maintenance, security systems, fire control systems.

8.13.6 Network Systems

Additions, modifications, deletions to lines, switches, routers, network access, controllers, servers, protocol converters. Software components either distributed or centralized, router software, printing routines, servers.

8.13.7 Operating procedures

Changes in equipment downtime schedules, planned system outages, changes in delivering services, or changes to service levels.

8.13.8 Web Applications

Requests for new functionality, maintenance, and bug fixes. This also includes requests to fix system crashes, unplanned downtimes, and sluggish performance. Requests for new functionality must also go through the IT Intake and Development Process as documented in the Intake and Development Procedure.

8.13.9 Workstations

Changes in hours of availability, hardware configurations, operating systems, utilities, applications including release levels or versions, installations or de-installations of systems.

9.0 Password Policy

Control Number:

Control Objective:

Item Name:

Task:

9.1 Overview

All HillSouth employees (including contractors and vendors with access to HillSouth systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

9.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

9.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any HillSouth facility, has access to the HillSouth network, or stores any non-public HillSouth information.

9.4 Policy

9.4.1 General

- All system-level passwords (e.g., root, administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

9.4.1.1 Password Protection Standards

Do not use the same password for HillSouth accounts as for other non-HillSouth access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various HillSouth access needs.

Do not share HillSouth passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential HillSouth information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message

- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call the Help Desk.

Do not use the "Remember Password" feature of Windows or applications (e.g., Internet Explorer, Outlook, Netscape, etc.).

Again, do not write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system (including Blackberrys or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident and change all passwords.

Administrative password cracking or guessing may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

9.4.1.2 Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

9.4.1.3 Use of Passwords and Shared Keys for Remote Access Users

Access to the HillSouth network via remote access (VPN) is to be controlled using either password authentication or a shared key system managed by a VPN client.

9.4.2 Active Directory

- Change passwords every 42 days (except system-level passwords which must be changed at least quarterly).
- Users cannot reuse any of their last 24 passwords.
- Password must be a minimum of 7 characters; it must contain one capital letter or special character and at least one number.

9.4.3 Connections

- New users receive a temporary password that needs to be changed every 90 days
- Users cannot reuse their previous password when prompted to change it

- Passwords must be a minimum of 6 characters; passwords require at least one capital letter and one number
- Passwords are encrypted using a 128 bit RC4 stream cipher during transmission to the server and are stored in the database using a secure 160-bit SHA hash value. This secure hash means that although passwords may be reset by an administrator they can never be retrieved from the database.

9.4.4 Oracle Financials

- New users receive a temporary password that needs to be changed when they first log in
- Users must change their passwords every 60 days and cannot reuse the last 5 iterations of their passwords
- Passwords must be a minimum of 7 characters; passwords are case sensitive, require at least an uppercase letter and a number, and do not allow repeated characters,

9.5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9.6 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator).

10.0 Database Password Policy

Control Number:

Control Objective:

Item Name:

Task:

10.1 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of HillSouth's networks.

Computer programs running on HillSouth's networks often require the use of one of the internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

10.2 Scope

This policy applies to all software that will access a HillSouth, multi-user production Oracle database.

10.3 Policy

10.3.1 General

In order to maintain the security of HillSouth's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

10.3.2 Specific Requirements

10.3.2.1 Storage of Database User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.

- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the Password Policy.

10.3.2.2 Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- The storage of user's database credentials must be physically separated from the other areas of the code, e.g., the credentials must be in a separate source file.
- For languages that execute from source code, the credentials source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

10.3.2.3 Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the Password Policy.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

10.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10.5 Definitions

Term	Definition
Computer language	A language used to generate programs.
Credentials	Something a user knows (e.g., a password or pass phrase), and/or something that identifies a user as being present for authentication (e.g., a user name, a fingerprint, voiceprint, retina print).
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.

Term	Definition
Hash	An algorithmically generated number that identifies a datum or its location.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

11.0 Email Retention Policy

Control Number:

Control Objective:

Item Name:

Task:

11.1 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction. Questions about the retention of a specific piece of information should be addressed to a manager. Questions about these guidelines should be addressed to the Internal Help Desk.

11.2 Scope

IT provides the infrastructure for departments to retain emails. Each department is responsible for retaining its own emails according to its own policies.

11.3 Policy

11.3.1 Categories of Correspondence

Categories of correspondence that users should use when considering whether to retain an email include:

- Administrative – clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations.
- Fiscal – information related to revenue and expense for the company.
- Ephemeral – personal email, requests for recommendations or review, email related to product development, updates and status reports.
- General – information that relates to customer interaction and the operational decisions of the business.
- Protected Health Information – any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

11.3.2 Instant Messenger Correspondence

HillSouth Instant Messenger correspondence may be saved with logging function of Instant Messenger or at the server level for Spark users. Important conversations should be copied and saved in a file on a backed up drive or in an email.

11.3.3 Server Email Retention and Backup

HillSouth does not purge the email server of old emails. Symantec Backup Exec runs a weekly full backup of all stored emails every Friday at 12am. Two weeks worth of full backups are kept at all times. Incremental backups are run every day, except Friday, at 12am. Two days worth of incremental backups are kept at all times.

11.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11.5 Definitions

Term	Definition
Approved Electronic Mail	Includes all mail systems supported by Systems & Security. For business needs that require the use of other systems, contact the appropriate support organization.
Approved Instant Messenger	Microsoft IM and Spark are the only IM clients approved for use on HillSouth's computers.
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac's and PCs, this includes using passwords on screensavers.
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of HillSouth.

12.0 Encryption Policy

Control Number:

Control Objective:

Item Name:

Task:

12.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

12.2 Scope

This policy applies to all HillSouth employees and affiliates.

12.3 Policy

Proven, standard algorithms such as 3DES, RSA, and RC5 should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, PGP Corporation's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. HillSouth's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question. Be aware that the U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

12.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12.5 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

13.0 Extranet Policy

Control Number:

Control Objective:

Item Name:

Task:

13.1 Purpose

This document describes the policy under which third party organizations connect to HillSouth networks for the purpose of transacting business related to HillSouth.

13.2 Scope

Connections between third parties that require access to non-public HillSouth resources fall under this policy, regardless of whether a T1 circuit, cable or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for HillSouth or to the Public Switched Telephone Network does NOT fall under this policy.

13.3 Policy

13.3.1 Pre-Requisites

13.3.1.1 Security Review

All new extranet connectivity will go through a security review by IT management. The reviews are to ensure that all access matches the business requirements in the best possible way, and that the principle of least required access is followed.

13.3.1.2 Third Party Connection Agreement

All new connection requests between third parties and HillSouth require that the third party and HillSouth representatives agree to and sign the Third Party Agreement. This agreement must be signed by the HillSouth executive management as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group.

13.3.1.3 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by IT management. Typically this function is handled as part of the Third Party Agreement.

13.3.1.4 Point of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet organization must be informed promptly.

13.3.2 Establishing Connectivity

Sponsoring Organizations within HillSouth that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage IT management to address security issues inherent in the project.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will HillSouth rely upon the third party to protect HillSouth's network or resources.

13.3.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying IT management when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

13.3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within HillSouth must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct HillSouth business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct HillSouth business necessitate a modification of existing permissions, or termination of connectivity, IT management will notify the POC or the Sponsoring Organization of the change prior to taking any action.

13.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

13.5 Definitions

Term	Definition
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional T1, cable, or via VPN/Encryption technologies.
Sponsoring Organization	The HillSouth organization who requested that the third party have access into HillSouth.
Third Party	A business that is not a formal or subsidiary part of HillSouth.

14.0 Incident Handling Policy

Control Number:

Control Objective:

Item Name:

Task:

14.1 Overview

HillSouth is increasingly dependent on data and network resources. Proper detection and response to incidents that may impact the integrity, confidentiality or availability of these resources is critical to the operation of the company. Such incidents include, but are not limited to: virus outbreaks, physical or remote security breaches, denial-of service attacks, and other exploited vulnerabilities.

The following standards were developed by HillSouth to prepare those employed by or affiliated with the company to properly detect and respond to incidents of any kind. Individuals are encouraged to implement any additional plans they deem necessary. These recommendations should not be used to reduce the level of preparedness that may already exist.

These minimum standards apply to all HillSouth departments and affiliates, as well as contractors and vendors handling HillSouth's systems or data. They represent the recommended minimum planning and cooperative efforts necessary to ensure the best incident detection and response possible.

14.2 Security Incident Detection

HillSouth users and administrators should be alert for symptoms that indicate and intrusion into their systems. The following points are helpful in detecting intrusions:

Be suspicious of unusual activity – unusual computer or network activity can be an indicator of a virus, attack, or intrusion. Activities and symptoms to look for include:

- Excessive virus warnings or personal firewall pop-up messages
- Unexpected system reboots and/or sudden degradation of system performance
- Unauthorized new user accounts or altered passwords
- New directories or files, often with unusual names such as "..." or " .."
- Modification or defacement of web sites
- New open network ports on a system
- Unexpectedly full disk drives

Listen to complaints received from others – comments or emails claiming suspicious activity from a computer may indicate the machine is infected or has been compromised and may actively be attacking other computers.

Be aware of the physical environment – access to secure areas at HillSouth is restricted, and situations to be aware of include:

- Unauthorized personnel in secure areas
- Unknown users at a computer
- Missing or moved equipment
- Open or unlocked doors that are normally secured

HillSouth regularly reviews server logs through Kiwi Enterprise Syslog Server – log files are invaluable in detecting and tracking attempted intrusions and other suspicious activity. To maximize the value of logs, the HillSouth Network Administrator:

- Ensures that a very high level of logging is enabled
- Checks logs regularly for suspicious activities and entries
- Monitors email alerts for suspicious activities
- Looks for missing time spans in logs
- Checks for repeated login failures or account lockouts
- Investigates unexpected system reboots
- Scans corporate antivirus logs for alerts and threat warnings

14.3 Incident Response

All HillSouth system users should immediately report suspicious activity to the Internal Help Desk. Administrators will refer to HillSouth's Incident Response Guidelines for technical assistance in investigating the incident.

This policy is applicable to any incident that occurs at HillSouth, including but not limited to security incidents, physical injury, theft, property damage, denial of service, threats, harassment and/or other criminal offenses involving individual user accounts, forgery and/or misrepresentation.

14.4 Definitions

Term	Definition
Incident	Any adverse event which compromises some aspect of HillSouth computer or network functionality/security, or business operations.
Vulnerability	A characteristic piece of technology which can be exploited to perpetrate a security incident.

15.0 Incident Response Guidelines

Control Number:

Control Objective:

Item Name:

Task:

15.1 Overview

HillSouth computer users must be prepared to respond properly when a security incident occurs. HillSouth takes a proactive approach to incident handling. A solid plan of attack for different types of security incidents is crucial to the continuance and/or restoration of normal operations at HillSouth.

15.2 Purpose

The purpose of this document is to provide security personnel and administrators with guidelines for incident handling at HillSouth.

15.3 Scope

These minimum standards apply to all HillSouth departments and affiliates, including contractors and vendors handling HillSouth systems or data.

15.4 Guidelines

Responses to specific incidents may include:

15.4.1 Incident Evaluation and response

- Check all systems for new or modified accounts
- Review log files for abnormal entries or missing time spans
- Look for modifications made to system software and/or configuration files
- Scan system for new binaries (including user directories)
- Check other local systems and related remote systems
- Change system password(s)
- Clean and/or reformat the system as appropriate

15.4.2 Incident Reporting

- Fill out a Test Track form in accordance with 8.7 Submission of a Change Request
- Contact the Internal Help Desk immediately to discuss the nature of the incident

16.0 Information Sensitivity Policy

Control Number:

Control Objective:

Item Name:

Task:

16.1 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of HillSouth without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that employees can take to protect HillSouth Confidential information (e.g., HillSouth Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to a manager. Questions about these guidelines should be addressed to Human Resources.

16.2 Scope

All HillSouth information is categorized into two main classifications:

- HillSouth Public
- HillSouth Confidential
    - Client Confidential (subset of HillSouth Confidential)

HillSouth Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to HillSouth, Inc.

HillSouth Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in HillSouth Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of HillSouth Confidential information is "Client Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to HillSouth by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into HillSouth's network to support our operations.

HillSouth personnel are required to secure HillSouth Confidential (as well as subset Client Confidential) information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager immediately.

16.3 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as HillSouth Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the HillSouth Confidential information in question.

Marking is at the discretion of the owner or custodian of the information. Even if no marking is present, HillSouth information is presumed to be "HillSouth Confidential" unless expressly determined to be HillSouth Public information by a HillSouth employee with authority to do so.

16.3.1 Minimal Sensitivity - "HillSouth Public": General corporate information; some personnel and technical information

Access: HillSouth employees, contractors, people with a business need to know.

Distribution within HillSouth: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of HillSouth internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on HillSouth premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

16.3.2 More Sensitive - "HillSouth Confidential": Business, financial, technical, and most personnel information

Access: HillSouth employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within HillSouth: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of HillSouth internal mail: Sent via U.S. mail or approved private carriers.

16.3.3 Electronic distribution: No restrictions to approved recipients within HillSouth, but should be encrypted or sent via a private link to approved recipients outside of HillSouth premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In disposal bins on HillSouth premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

16.3.4 Most Sensitive - Elements of "HillSouth Confidential" and all "Client Confidential": Trade secrets & marketing, operational, personnel, financial, source code, & technical Information integral to the success of our company and all Client Confidential Data

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that HillSouth Confidential information is very sensitive, consider labeling the information with "HillSouth Internal: Registered and Restricted", "HillSouth Eyes Only", "HillSouth Confidential" or similar labels as deemed by the affected individual business unit or department. Once again, this type of HillSouth Confidential information need not be marked, but users should be aware that this information is extremely sensitive and must be protected as such.

Access: Only those individuals (HillSouth employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within HillSouth: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of HillSouth internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within HillSouth, but all "Confidential" information must be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In disposal bins on HillSouth premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

16.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

16.5 Definitions

Terms	Definitions

Terms	Definitions
Appropriate measures	To minimize risk to HillSouth from an outside business connection, HillSouth computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access HillSouth corporate information, the amount of information at risk is minimized.
Configuration of HillSouth-to-other business connections	Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.
Approved Electronic File Transmission Methods	Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential	Special envelopes are not required. Put the document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes all mail systems supported by the Network Administrator. These include, but are not necessarily limited to Microsoft Exchange and Outlook. For business needs that require the use of other mailers contact the appropriate support organization.
Approved Encrypted email and files	Techniques include the use of PGP or GPG. DES encryption is available via many different public domain packages on all platforms. Please contact the Help Desk regarding approved encryption methods.
Company Information System Resources	Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
Expunge	To reliably erase or expunge data on a PC, a separate program must overwrite data. Otherwise, the PC's normal erasure routine keeps the data intact until overwritten.
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On PCs, this includes using passwords on screensavers.

Terms	Definitions
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of HillSouth.
Encryption	Secure HillSouth Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult the Help Desk for further guidance.
Physical Security	Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state. Methods of accomplishing this include having a domain username and password to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or keep it in person. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet. No information, equipment, or software belonging to HillSouth shall be removed from the premises without express authorization from executive management.
Private Link	A Private Link is an electronic communications path that HillSouth has control over its entire distance. For example, all HillSouth networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. Connections to employee's homes are private links.

17.0 Media Disposition Policy

Control Number:

Control Objective:

Item Name:

Task:

17.1 Purpose

This document provides specific guidance on methods, processes and procedures to ensure no data remains on removable storage devices that are to be permanently removed from HillSouth.

17.2 Methods for media sanitization and clearing

Overwriting is the process of replacing information (data) with meaningless data in such a way that meaningful information cannot be recovered from a device. The HillSouth technician performing the overwriting will have suitable technical expertise and will be responsible for certifying that the process has been successfully completed.

Destruction of a device is the process of physically damaging a medium so that it is not usable in a computer and so that no known exploitation method can retrieve data from it.

Clearing data (deleting files) simply removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing HillSouth controlled storage media.

17.3 Disposition

Storage devices may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

18.0 Network Documentation Policy

Control Number:

Control Objective:

Item Name:

Task:

18.1 Overview

This network documentation policy is an internal HillSouth policy and defines the requirements for network documentation. This policy defines the level of network documentation required such as documentation of which switch ports connect to what rooms and computers. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

18.2 Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy complements disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

18.3 Documentation

The network structure and configuration shall be documented and provide the following information:

1. IP addresses of all devices on the network with static IP addresses.
2. Server documentation on all servers as outlined in the "Server Documentation" document.
3. Network drawings showing:
    1. The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
    2. The various security zones on the network and devices that control access between them.
    3. The interrelationship between all network devices showing lines running between the network devices.
    4. All subnets on the network and their relationships including the range of IP addresses on all subnets and subnet mask information.
    5. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.
4. Configuration information on all network devices including:
    1. Switches
    2. Routers
    3. Firewalls
5. Configuration includes but is not limited to:

    1. IP Address
    2. Subnet mask
    3. Default gateway
    4. DNS server IP addresses for primary and secondary DNS servers.
6. Network connection information including:
    1. Type of connection to the internet or other WAN/MAN including cable, T1, or fiber.
    2. Provider of internet/WAN/MAN connection and contact information for sales and support.
    3. Configuration information including subnet mask, network ID, and gateway.
    4. Physical location of where the cabling enters the building and circuit number.
7. DHCP server settings showing:
    1. Range of IP addresses assigned by all DHCP servers on all subnets.
    2. Subnet mask, default gateway and DNS server settings assigned by all DHCP servers on all subnets.
    3. Lease duration time.

18.4 Access

IT Department Management have full access to all network documentation. IT Department Management shall have the ability to read and modify network documentation. Designated enterprise security staff shall have access to read and change network documentation but those not designated with change access cannot change it.

18.5 Change Notification

Appropriate groups of people shall be notified through email when network changes are made including:

1. Reboot of a network device including switches, routers, and firewalls.
2. Upgrades to any software on any network device.
3. Additions of any software on any network device.
4. Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:
    1. DHCP
    2. DNS
    3. Domain controllers

18.6 Documentation Review

The Network Administrator shall ensure that network documentation is kept current by performing a quarterly review of documentation or designating a staff member to perform a review. The Test Track requests within the last quarter should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings are reviewed to determine whether there were any network changes made to support the project.

18.7 Storage Locations

Network documentation is kept either in written form or electronic form in a minimum of two places. It is kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help reconstruct the IT infrastructure. Information in both facilities is updated monthly at the time of the documentation review.

19.0 Patch Management and Systems Update Policy

Control Number:

Control Objective:

Item Name:

Task:

19.1 Patch Management Overview

Patches are usually released for three reasons:

1) To fix faults in an application or operating system.
2) To alter functionality or to address a new security threat.
3) To change or modify the software configuration to make it less susceptible to attacks and more secure.

This policy establishes a patch management and systems update policy for all IT systems, devices and appliances, regardless of operating system or platform.

19.2 Policy

HillSouth has established and implemented an automated company-wide system of patch management for all IT systems, devices and appliances, regardless of operating system or platform. This consists of clearly assigned specific responsibilities for the Systems Administrator. All authorized personnel are trained in system administration to include patch management techniques. Patch management is used in conjunction with the normal vulnerability scanning efforts. HillSouth uses automated patch management software (Microsoft WSUS) to keep patches current, and certifies that system patches have been applied using the Microsoft WSUS logging methods. These logs and reports will be completed on an ongoing basis and kept on file for audit and/or review.

Patches are tested on non-production systems prior to installation on all production systems. In addition, HillSouth maintains an organizational hardware and software inventory and an electronic database (WSUS) of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to external entities.

19.3 Policy Exception Requirements

Exceptions to policy will be considered only in terms of implementation timeframes - exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature. Interim exceptions cannot extend beyond the fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. The System Administrator will monitor all approved exceptions.

19.4 Procedures

Although the National Institute of Standards and Technology (NIST) recommends that companies establish a "Patch and Vulnerability Group", this is optional in establishing a patch management program. HillSouth has established a program utilizing the most efficient and effective way to manage patches possible given their environment. At a minimum, the following duties and responsibilities have been delegated to the System Administrator:

19.4.1 Create and Maintain an Organizational Hardware and Software Inventory to include a Patch Management Database containing:

- Hardware equipment and software packages
- Version numbers of those packages within the organization
- Patches that apply to this equipment and patch status.

Most automated patch management programs (Microsoft WSUS for example) provide this functionality and are preferred over manual patch solutions. This database enables the Systems Administrator to monitor for information about vulnerabilities and patches that correspond to the hardware and software within the inventory. Specific attention is given to those software packages that are used on important servers or that are used by a large number of systems. This includes any connected resources and any external resources that are used for official HillSouth business. This database is updated in a timely manner when a system is installed or upgraded. Post-patch distribution updates to the database are executed immediately following any patching exercise.

19.4.2 Identify Newly Discovered Vulnerabilities and Security Patches

The Systems Administrator is responsible for proactively monitoring security sources for vulnerabilities and patches that correspond to the software within the organizational hardware and software inventory. A variety of sources are monitored to ensure that they are aware of all the newly discovered vulnerabilities.

When a vulnerability has no satisfactory patch, the Systems Administrator presents alternative risk mitigation approaches to management and supports that management decision by testing, documenting, and coordinating implementation with the appropriate system. Most automated solutions will perform the bulk of this requirement; any devices not covered by the automated system will be recorded manually in the database.

19.4.3 Prioritize Patch Application

The Systems Administrator prioritizes the set of known patches. The criticality of a patch is a risk-based decision utilizing standard elements such as Probability and Consequence. Consideration of consequences usually extends beyond a system's logical boundaries and requires a broader approach in weighing this factor. For example, HillSouth will always consider Operating System (OS) Patches that are deemed critical by the software vendor as critical. A distinction is made between servers and end-user systems when making patching recommendations because often it is more important to patch servers on a routine schedule before end-user systems. Care is taken to ensure that the automatic patch distribution solution targets the correct machines. Patches deemed critical are tested and installed on applicable systems within calendar 30 days of general release. Engineering patches (i.e. beta service packs) are generally avoided unless the criticality is extremely high and the general availability release date poses a significant risk to the target systems.

19.4.4 Verify Patch Installation Through Network and Host Vulnerability Scanning

The Systems Administrator performs monthly network and host vulnerability scanning to identify systems that have not been patched as required. Scanning results will provide the Systems Administrator with another data source for new vulnerabilities and patches. However, network and host vulnerability scanners do not check for every known vulnerability and cannot be relied on as the sole source of vulnerability information.

19.4.5 Identify Patches and Vulnerabilities Associated with Software On Local Systems

As previously mentioned, the organizational software inventory and patch database may not contain all software used by HillSouth. All patches applied or vulnerabilities identified will require correction and testing in accordance with the procedures outlined above.

19.5 Corporate Responsibilities

19.5.1 The Chief Executive Officer

- Supports the establishment and maintenance of patch management policy and procedures within HillSouth
- Ensures that funding and personnel are provided to effectively maintain enterprise-wide patch management solutions

19.5.2 The Systems Administrator

- Develops and publishes policy and procedural guidance on patch management
- Provides enterprise-wide tools to assist in compliance efforts
- Monitors patch management on an enterprise-wide basis
- Provides advice and guidance in effectively patching systems and eliminating vulnerabilities
- Supports exception requests from the patch management policy to ensure that appropriate security protection is provided
- Implements an internal program for patch management on all IT systems
- Ensures that all IT professionals are trained and made aware of this policy
- Clearly assigns authorized personnel specific patch management and vulnerability correction responsibilities
- Employs an approved automated patch management solution to facilitate compliance with this policy and to promote efficiency for all systems, and applies patch management solutions to in-house applications and monitors the status of those systems
- Reports patch management status monthly
- Requests a formal exception through the established process for any systems which are not compliant within 90 days
- Stays current with new patch management policy, procedures, and enterprise wide solutions
- Acts as a Point of Contact (POC) for security to provide guidance and assistance to any individuals designated patch management responsibilities

20.0 Remote Access Policy

Control Number:

Control Objective:

Item Name:

Task:

20.1 Purpose

The purpose of this policy is to define standards for connecting to HillSouth's network from any host. These standards are designed to minimize the potential exposure to HillSouth from damages that may result from unauthorized use of HillSouth's resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical HillSouth's internal systems, etc.

20.2 Scope

This policy applies to all HillSouth employees, contractors, vendors and agents with a HillSouth-owned or personally-owned computer or workstation used to connect to the HillSouth network. This policy applies to remote access connections used to do work on behalf of HillSouth, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, T1, cable modems, DSL, VPN (using an encrypted VPN client), etc.

20.3 Policy

20.3.1 General

1. It is the responsibility of HillSouth's employees, contractors, vendors and agents with remote access privileges to HillSouth's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to HillSouth's network.
2. General access to the Internet for recreational use by immediate household members through the HillSouth network on personal computers is not permitted for employees. The HillSouth employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of HillSouth's network:
    1. Acceptable Encryption Policy
    2. Virtual Private Network (VPN) Policy
    3. Wireless Communications Policy
    4. Acceptable Use Policy
4. For additional information regarding HillSouth's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., contact the Help Desk.

20.3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication or shared keys. For information on creating a strong password see the Password Policy.
2. At no time should any HillSouth employee provide their login or email password to anyone, not even family members.
3. HillSouth employees and contractors with remote access privileges must ensure that their HillSouth-owned or personal computer or workstation, which is remotely connected to HillSouth's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. HillSouth employees and contractors with remote access privileges to HillSouth's corporate network must not use non-HillSouth email accounts (i.e., Hotmail, Yahoo, AOL, GMail), or other external resources to conduct HillSouth business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated lines configured for access to the HillSouth network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling is not permitted at any time.
7. Non-standard hardware configurations must be approved by System Administrator, and must use approved security configurations for access to hardware.
8. All hosts that are connected to HillSouth internal networks via remote access technologies must use the most up-to-date anti-virus software and definitions, and this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.
9. Personal equipment that is used to connect to HillSouth's networks must meet the requirements of HillSouth-owned equipment for remote access.
10. Organizations or individuals who wish to implement non-standard Remote Access solutions to the HillSouth production network must obtain prior approval from the System Administrator.

20.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

20.5 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 5 Mbps.

Term	Definition
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a HillSouth-provided Remote Access home network, and connecting to another network, such as a spouse's remote access.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Remote Access	Any access to HillSouth's corporate network through a non-HillSouth controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-HillSouth network (such as the Internet, or a home network) from a remote device (PC, PDA, etc.) while connected into HillSouth's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

21.0 Virtual Private Network (VPN) Policy

Control Number:

Control Objective:

Item Name:

Task:

21.1 Purpose

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the HillSouth corporate network.

21.2 Scope

This policy applies to all HillSouth employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing a VPN to access the HillSouth network.

21.3 Policy

Approved HillSouth employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of a VPN, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying any associated fees. Further details may be found in the Remote Access Policy.

Additionally,

1) It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to HillSouth internal networks.
2) VPN use is to be controlled using strong password authentication and shared key.
3) When actively connected to the corporate network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4) Dual (split) tunneling is NOT permitted; only one network connection is allowed at a time.
5) VPN gateways (through SonicWALL) will be set up and managed by the System Administrator.
6) All computers connected to HillSouth internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (Symantec Endpoint Protection); this includes personal computers.
7) Users of computers that are not HillSouth-owned equipment must configure the equipment to comply with HillSouth's VPN and Network policies.
8) Only the authorized encrypted VPN client may be used for VPN access.
9) By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of HillSouth's network, and as such are subject to the same rules and regulations that apply to HillSouth-owned equipment, i.e., their machines must be configured to comply with HillSouth's Security Policies.

21.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

21.5 Definitions

Term	Definition
Dual (split tunneling)	The practice of connecting to HillSouth network resources via VPN while simultaneously connecting to a second tunnel (i.e. the internet).

22.0 Removable Media Policy

Control Number:

Control Objective:

Item Name:

Task:

22.1 Overview

Removable media can be classified as any portable device that can be used to store and/or move data. Media devices can come in various shapes and forms, including USB memory sticks, floppy disks, read/write compact disks and DVDs, PDA storage cards, magnetic tapes and cassettes – essentially anything that can be copied, saved, and/or written to which can then be taken away and restored on another computer.

By design, removable media create their own security vulnerabilities – they provide the means to conveniently transport up to several gigabytes of data from one computer or network to another. The most salient vulnerabilities being:

1) Most forms of removable media require no form of authentication, password protection, or configuration to install or use and they can make use of "plug and play" technologies and generally do not require any administrator privileges to install.
2) Unauthorized disclosure of sensitive data could occur if an item of removable media fell into the wrong hands.
3) In addition to their authorized data, users may also inadvertently transport (and therefore introduce) malicious software on to HillSouth's systems.
4) The nature and tangible size of removable media is such that they are also prone to accidental loss and/or theft.

22.2 Restrictions for the Management of Removable Media

1) Only HillSouth owned and managed removable media should be used with HillSouth systems.
2) It is not permissible to use HillSouth owned media on personal computers or other devices that do not have an official connection to HillSouth networks.
3) High sensitivity data must be protected to 128bit encryption levels when stored on removable media. If it is not possible to achieve this level of encryption, then its storage is prohibited.
4) Removable media should only be used to transport or store data when other more secure means (internal email or network shares) are not available.
5) If any item of removable media is no longer required by HillSouth, it must be destroyed by approved secure means. This is only to be carried out by the Help Desk.
6) When transferring data from outside of HillSouth, extreme caution must be taken, as the potential impact of a malicious software attack on HillSouth's systems could be severe.
7) Any loss or theft of any item of removable media must be reported immediately to the Help Desk so that the level of compromise can be assessed, and necessary efforts can be made for recovery.

22.3 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

23.0 Risk Assessment Policy

Control Number:

Control Objective:

Item Name:

Task:

23.1 Purpose

To document how the Network Administrator performs periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability and initiates appropriate remediation.

23.2 Scope

Risk assessments can be conducted on any entity within HillSouth or any outside entity that has signed a Third Party Agreement with HillSouth. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

23.3 Policy

The execution, development and implementation of remediation programs is the joint responsibility of the Network Administrator and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Network Administrator in the development of a remediation plan.

23.4 Risk Assessment Process

Describe process to complete risk assessments on a periodic basis, key players involved and tests performed.

23.5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

23.6 Definitions

Terms	Definitions
Entity	Any business unit, department, group, or third party, internal or external to HillSouth, responsible for maintaining HillSouth assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of HillSouth's key information assets and systems. The Network Administrator is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

24.0 Server Documentation Policy

Control Number:

Control Objective:

Item Name:

Task:

24.1 Overview

This policy is an internal HillSouth policy and defines the requirements for server documentation. This policy defines the level of server documentation required such as configuration information and services that are running. It defines who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers.

24.2 Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

24.3 Documentation

For every server on a secure network, there is a list of items that must be documented and reviewed on a regular basis to keep a private network secure. This list of information about every server should be created as servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server.
4. Hardware components of the system including the make and model of each system.
5. List of essential software running on the server including operating system, programs, and services running on the server.
6. Configuration information about how the server is configured including:
    1. Event logging settings
    2. Configuration of any security lockdown tool or setting
    3. Account settings
    4. Configuration and settings of software running on the server.
7. Types of data stored on the server.
8. The sensitivity of data stored on the server.
9. Data on the server that should be backed up along with its location.
10. Users or groups with access to data stored on the server.
11. Administrators on the server with a list of rights of each administrator.

12. The authentication process and protocols used for authentication for administrators on the server.
13. Latest patch to operating system.
14. Disaster recovery plan and location of backup data.

24.4 Access Control

The HillSouth Network Administrator and Technical Communications have full read and change access to server documentation for the server or servers they are tasked with administering.

24.5 Change Notification

The network administration staff, application developer staff, and executive management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

24.6 Documentation Review

HillSouth's Network Administrator ensures that server documentation is kept current by performing a quarterly review of documentation or designating a staff member to perform a review. The Test Track requests within the last quarter should be reviewed to help determine whether any server changes were made. Also any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

24.7 Storage Locations

HillSouth's server documentation is kept either in written form or electronic form in a minimum of two places. It is kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the HillSouth IT infrastructure. Information in both facilities is updated monthly at the time of the documentation review.

25.0 Server Security Policy

Control Number:

Control Objective:

Item Name:

Task:

25.1 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by HillSouth. Effective implementation of this policy will minimize unauthorized access to HillSouth proprietary information and technology.

25.2 Scope

This policy applies to server equipment owned and/or operated by HillSouth, and to servers registered under any HillSouth-owned internal network domain.

This policy is specifically for equipment on the internal HillSouth network.

25.3 Policy

25.3.1 Ownership and Responsibilities

All internal servers deployed at HillSouth must be operated by the Network Administrator. Approved server configuration guides must be established and maintained by the Network Administrator, based on business needs and approved by HillSouth. The Network Adminstrator should monitor configuration compliance and implement an exception policy tailored to the server's environment. The Network Adminstrator must establish a process for changing the configuration guides, which includes review and approval by HillSouth.

- Servers must be documented according the Server Documentation Policy.
- Configuration changes for production servers must follow the appropriate change management procedures.

25.3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved HillSouth guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

- Always use standard security principles of least required access to perform a function.
- Do not use the administrator account when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSL or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

25.3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved to the Syslog servers.
- Security-related events will be reported to the Network Administrator, who will review logs and report incidents. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

25.3.4 Compliance

- Audits will be performed on a regular basis by HillSouth.
- Audits will be managed by the Network Administrator. The Network Administrator will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

25.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

25.5 Definitions

Term	Definition
DMZ	Demilitarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal HillSouth Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

26.0 Source Code Control Policy

Control Number:

Control Objective:

Item Name:

Task:

26.1 Revision Control

Source code revision control is accomplished utilizing a Subversion server whose data is kept on a redundant SAN and replicated daily to minimize the possibility of data loss. Subversion is an open-source revision control software package, maintained by the well-respected Apache Software Foundation, which keeps a complete history of all changes made to the software application. Using a Subversion client, authorized users can commit changes to the code repository and roll back previous changes if the need arises. Users may also compare the differences between separate revisions of the application to see everything that changed from one version to the next. Access to the code repository is limited using folder-level permissions which are customized for each authorized user.

A separate release branch is maintained in the Subversion repository which allows revisions to be selectively released as they are deemed stable after being fully tested and accepted by all affected users. The production package is built from this release branch, which only the change manager has write access to, so developers have no way of directly releasing their own code. The software manager will merge changes from the main code trunk to the release branch only after the Business Analysis and Quality Assurance teams advise him that the change is authorized to be deployed. This release authorization is documented in an official release communication which is copied to all affected parties.

Revisions are not released individually; all revisions for a given project will be released at the same time. Projects are tracked using the TestTrack issue management software package. Each project is given a unique identifier in TestTrack which is used to track the project from inception to completion. All code committed to the Subversion repository requires an associated TestTrack issue. To identify all software revisions associated with a single TestTrack issue, we associate the TestTrack IDs with every committed revision using the following format:

- TT##### - Description of changes made goes here

When a given project is authorized for release, the change manager will merge all of the revisions associated with that project from the code trunk to the release branch in a single atomic action. This allows the change to easily be removed from the production build in the unlikely event that any unforeseen complications arise.

26.2 Source Control Life Cycle

The life-cycle of a single issue is as follows:

1. TestTrack issue is created after Business Analysis team verifies business needs of project and Software Development team verifies changes are required
2. Issue is assigned to a developer who creates a development branch that starts as a copy of the code trunk and tracks all changes the developer makes for the issue

3. Developer completes development of project, merges changes from their development branch into the code trunk and assigns the issue to the release manager
4. Release manager creates a test build from the code trunk, releases the test build to the testing site and assigns the issue to the Quality Assurance team
5. After Quality Assurance team verifies changes are working as intended the issue is assigned to the Business Analysis team and users are chosen for acceptance testing
6. Once all testing and acceptance is completed, project is assigned back to the release manager and is added to a scheduled release
7. All affected parties are notified of the release date which is to be no sooner than 30 days from completion of all testing
8. When the scheduled release date arrives the projects slated for release are merged into the release branch by the release manager who then builds the new version of the application
9. During scheduled downtime the night of the release the new version of the application is deployed to the production servers by the change manager and the TestTrack issue is closed

27.0 Wireless Communication Policy

27.1 Purpose

This policy prohibits access to HillSouth networks via unsecured wireless communication mechanisms.

27.2 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of HillSouth's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to HillSouth's networks do not fall under the purview of this policy.

27.3 Policy

27.3.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by HillSouth's Network Administrator. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with HillSouth's Help Desk.

27.3.2 Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations.

27.3.3 VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication.

27.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

27.5 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

28.0 Third Party Access

28.1 Purpose

All consultants, contractors, vendors, and outside parties such as law firms, hereinafter referred to as "Third Party" or "Third Parties" who access data hosted by HillSouth must comply with this policy. All HillSouth Third Parties must secure against unauthorized network or physical access, damage or interference to HillSouth's business operations assets, including but not limited to confidential client information and IT resources. HillSouth Third Parties are subject to applicable requirements of this policy when they perform work for HillSouth or its clients. HillSouth Third Parties who violate this policy will be subject to termination of access and investigation and may result in breach of contract or other penalties.

28.2 Third Party Access General requirements

1. All Third Parties must sign a non-disclosure / confidentiality agreement.

2. Third Parties may only access network and system resources by approved methods.

3. Third Parties must ensure basic security methodologies are in place within their infrastructure (firewall, user access control, etc.).

4. Individuals working for Third Parties are not allowed to share accounts or passwords.

5. Third Parties must ensure that any device connecting to HillSouth's infrastructure be secured with basic security tools (anti-malware/virus software, firewalls, etc.).

6. In the event of a security incident, HillSouth reserves the right to request an audit of the third parties processes or methods leading to the incident.

7. Third party must report any known or suspected security-related incident to HillSouth immediately.

EMPLOYEE NAME:

EMPLOYEE SIGNATURE:

DATE: