Diamond Hands Holding Inc.
Policy and Planning Omnibus

Table of Contents

Policy

Enterprise Information Security Policy

Statement of Purpose:

This document will identify elements of a good security policy, explain the need for information security, identify the information security roles and responsibilities, and establish minimum information security practices for Dimond Hands Holding Inc computer resources and associated communication networks utilizing the DHHI enterprise network.

Information Security Elements:

Information security is defined as the protection of information and the systems and hardware that use, store, and transmit that information. Therefore, this policy is intended to give direction on accepted security practices designed to ensure information confidentiality, integrity, and availability of company assets by managing threats and reducing vulnerabilities.

Assets are defined, in this case, as items that are owned by the company, that have an assessed financial value. This would include computer hardware, software, information, and lines of communication coming into and leaving the company campus. Threats are defined as objects, people, or other entities that represent a risk of loss to an asset(s). Threats occur in several categories. These include:

1. Acts of human error or failure (Accidents, employee mistakes)
2. Compromises to intellectual property (Piracy, copyright infringement)
3. Deliberate acts of espionage or trespass (Unauthorized access)
4. Deliberate acts of information extortion (Blackmail of disclosure)
5. Deliberate acts of sabotage or vandalism (Destruction of information)
6. Deliberate acts of theft (Illegal confiscation of equipment)
7. Deliberate software attacks (Viruses, worms, denial-of-service)
8. Deviations in QOS from service providers (Power and WAN issues)
9. Forces of nature (Fire, flood, earthquake, lightning)
10. Technical hardware failures or errors (Equipment failure)
11. Technical software failures or errors (Bugs, unknown loopholes)
12. Technical obsolescence (Antiquated or outdated technology)

Vulnerabilities are defined as weaknesses or faults in a system or protection mechanism that exposes information to an attack or damage. Attacks are acts of intentional or unintentional attempt to compromise the information and/or the systems that support it

Need for Information Security:

The continued use of information technology resources throughout DHHI' working infrastructure has continued to evolve with the intent of improving services for our constituency. These improvements allow for rapid and efficient communication among various departments and often directly with the directors of the surrounding business community. Consequently, our constituency has become heavily dependent upon the availability of a reliable information technology infrastructure to meet its

business needs. Unfortunately, the "electronic highways" that facilitate our ability to instantaneously share information also creates vulnerabilities, potentially allowing unauthorized persons to gain access to DHHI resources. In order to control threats to information technology resources across the enterprise network and associated domains, a series of Information security instructions, entitled "INFORMATION SECURITY POLICY, INSTRUCTIONS, AND TECHNICAL STANDARDS," is established.

Information Security Roles & Responsibilities:

DHHI technology resources will proactively track threat activity and work to prohibit or correct such activity. Where unintentional unauthorized access is detected, the affected organization will be advised to correct exploitable vulnerabilities to prevent future occurrences. Where unauthorized access is determined to be intentional it will be assumed to be malicious and an appropriate response will be initiated. All DHHI faculty members, staff, students, contractors, agents or other individuals utilizing computer resources, data communication networks, or other information technology infrastructure resources owned or leased by DHHI, including any other state agencies having electrical connectivity to the network are subject to this policy.
Additionally, any remote access, such as dial up connections, personal Internet Service Provider access or VPN connection, onto the DHHI enterprise network or associated domains will have the same effect as direct access via DHI provided equipment or facilities.

General Policy Elements:

1) Protection of Information:
Policy:Information must be protected in a manner commensurate with its sensitivity, value, and criticality
Audience: Technical Staff

2) Use of Information:
Policy: DHHI computer and communications systems must be used for appropriate business purposes only, by authorized personnel. Audience: All

3) Information Handling, Access, & Usage:
Policy: All data and information sent over the DHHI enterprise network, and associated domain communications systems, are the property of DHHI.
Audience: All

4) Data & Program Damage Disclaimers:
Policy: DHHI is not held responsible for any loss or damage to data or software that results from its efforts to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems.
Audience: End Users

5) Legal Conflicts:
Policy: DHHI information security policies were drafted to meet or exceed existing federal and state laws and regulations. Any policy implemented by DHHI that is found to be in conflict with any existing laws or regulations should immediately be brought to the attention of the Chief Information Security Officer
Audience: End Users

6) Exceptions to Policies:
Policy: Exceptions to information security policies exist on occasion where a risk assessment examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the data owner or management, and where this form has been approved by both the Chief Information Security Officer and internal Audit Management.
Audience: Management

7) Non-enforcement:
Policy: Management's non-enforcement of any policy requirement does not constitute its consent.
Audience: End Users

8) Violation of the Law:

Policy: DHHI will prosecute violators of federal and state computer crime laws as laid out within the applicable laws.
Audience: End Users

9) Revocation of Access Privileges
Policy: DHHI reserves the right to revoke a user's information technology privileges at any time
Audience: End Users

10) Industry-Specific Information Security Standards:
Policy: DHHI information systems must employ industry specific information security standards
Audience: Technical Staff

11) Use of Information Security Policies and Procedures
Policy: All DHHI information security documentation, including, but not limited to, policies, standards, and procedures, must be classified as "Internal Use Only", unless expressly created for external business processes and partners. Audience: All

12) Authority Over Data:
Policy: DHHI reserves the right to examine all information transmitted through these systems. Examination of such information may take place without prior warning to the parties sending or receiving such information. Audience: All

13) Expectation of Privacy :
Policy: Staff, contractors, agents or other individuals should have no expectation of privacy associated with the information they store in or send through these systems; most files and documents maintained by DHHI are subject to public review under the Georgia Open Records Act. This includes computer files and other stored material regardless of the medium of storage. Audience: All

14) Mission Critical Systems Information Handling:
Policy: DHHI reserves the right to delete, summarize, or edit any information posted to, or transiting through, DHHI information systems. These systems are scarce, Company owned-resources designed to support mission critical Company activities and goals.
Audience: All

Review & Evaluation:

1) Review Period:

Policy: This policy and associated instructions requires a quarterly review by the Chief Information Officer's Departmental Directors or agents.
Audience: Management

2) Authority:
Policy: Authority to establish and enforce this policy and associated security policy documents is made by Chief Information Officer and Chief Information Security Officer.
Audience: Management

Reference:

The Georgia Computer Systems Protection Act (O.C.G.A. 16-9-90) specifies unlawful acts involving information resources and subsequent penalties upon conviction. As data residing or transiting DHHI networks and machines is held in great trust it must be afforded the greatest safeguards. Therefore, information security policy, instruction, processes, and standards created in furtherance of protecting DHHI Company information assets rely upon the Georgia computer Systems Protection Act (O.C.G.A 16-9-90) TO ENSURE COMPLIANCE. Violators may be prosecuted accordingly.

** Portions of this policy were copied and or modified from tables 4-1 and 4-2 (pages 111-115) of Management of Information Security by Dr. Michael Whitman and Professor Herbert Mattord

Issue Specific Security Policies /System Security Policies

Anti-Virus:

1.0 Purpose

The purpose of this policy is to provide guidance for utilizing anti-virus software and preventing the introduction of malicious software or access to DHHI corporate owned systems, where corporate owned is defined as any system operating in a DHHI production environment on the company network, whether within the company owned facilities or issued to company agents or employees for use at remote locations for company business.

2.0 Scope

This policy applies to all DHHI employees and affiliates.

3.0 Policy

3.1 General Guidelines

Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available. 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 your Trash.

Delete spam, chain, and other junk email without forwarding, refer to DHHI'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 a floppy diskette from an unknown source for viruses before using it. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab 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.

3.2 Ownership

Responsibility will befall to IS/IT/InfoSec staff to verify current anti-virus revisions and maintain the corporate download website with current updates for corporate assets.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Macro	In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke.
Virus	virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document.

6.0 Revision History

Authentication & Authorization

Acceptable Encryption:

1.0 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.

2.0 Scope

This policy applies to all DHHI employees and affiliates.

3.0 Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate'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 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. DHHI'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 and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

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

5.0 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).

6.0 Revision History

Acceptable Use:

1.0 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to DHHI's established culture of openness, trust and integrity. InfoSec is committed to protecting DHHI's 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 DHHI. 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. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every DHHI 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.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at DHHI. These rules exist to protect the employee and DHHI. Inappropriate use exposes DHHI to risks including virus attacks, compromise of network systems and services, and legal action.

3.0 Scope

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

4.0 Policy

4.1 *General Use and Ownership*

While DHHI's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of DHHI. Because of the need to protect DHHI's network, management cannot guarantee the confidentiality of information stored on any network device belonging to DHHI.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by

departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
For security and network maintenance purposes, authorized individuals within DHHI may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.
DHHI reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

The user interface for 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 Human Resources policies. 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. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
Postings by employees from a DHHI email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DHHI, unless posting is in the course of business duties. All hosts used by the employee that are connected to the DHHI
Internet/Intranet/Extranet, whether owned by the employee or DHHI, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

5.0 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 that is disrupting production services).

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

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

5.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- 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 DHHI.
- 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 DHHI or the end user does not have an active license is strictly prohibited.
- 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.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a DHHI 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.
- Making fraudulent offers of products, items, or services originating from any DHHI account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

- 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.
- Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
- 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.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, DHHI employees to parties outside DHHI.

5.2 Email and Communications Activities

- 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).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- 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.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within DHHI's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DHHI or connected via DHHI's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.3 Blogging

- Blogging by employees, whether using DHHI’s property and systems or personal computer systems, is also subject to the terms and restrictions set

forth in this Policy. Limited and occasional use of DHHI's systems to engage in blogging is acceptable, if it is done in a professional and responsible manner, does not otherwise violate DHHI's policy, is not detrimental to DHHI's best interests, and does not interfere with an employee's regular work duties.

- Blogging from DHHI's systems falls under DHHI's Confidential Information Policy and Non-Discrimination and Anti-Harassment policy and is therefore subject to monitoring. As such, Employees are prohibited from revealing any Company confidential or proprietary information, trade secrets or any other material covered by Company's Confidential Information policy when engaged in blogging.

6.0 Enforcement

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

7.0 Definitions

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

8.0 Revision History

Password

1.0 Purpose

This policy provides the requirements for creating and retrieving usernames and passwords (i.e., credentials) for use by employees that require authentication and access resources on DHHI's network.

These credentials are meant to restrict access based on privileges as assigned by the IS/IT/InfoSec department and can be compromised when the credentials are improperly stored.

2.0 Scope

This policy applies to all users that will access DHHI resources, locally and through VPN/
remote access.

3.0 Policy

3.1 General

In order to maintain the security of DHHI's internal resources, access by user must be granted only after authentication on one of 3 Active Directory Domain Controller servers.

3.2 Specific Requirements

3.2.1 Username & Password Creation and Retention

- User names will consist of an employee's first initial and last name
- Passwords will be 8 to 12 characters in length
- Passwords will be a combination of upper and lower case alphanumeric values which can include common symbols.
- Passwords will be valid for 45 days
- A minimum of 12 passwords will be kept in the system's history, not to be repeated.
- Passwords must be stored using reverse encryption

3.2.2 Retrieval of User Names and Passwords

- If a user forgets his/her password, they should contact the DHHI technical support center (TSC) and request to have their password reset. The TSC will not have access to a user's password and therefore be unable to directly access a user's account without creating an audit log entry
- When a member of the DHHI TSC resets a user's password, an entry will be made into the system audit logs and said logs will be maintained for a period of one (1) year.
- User names consist of a standard format, as previously stated of first initial and last name. In the event of duplication, the user's first name initials will be used until such that duplication will not exist.

4.0 Enforcement

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

5.0 Definitions

9.0 **Term**	10.0 **Definition**
11.0 Credentials	12.0 Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
13.0 Entitlement	14.0 The level of privilege that has been authenticated and authorized. The privileges level at which to access resource

15.0 Executing body	16.0 The series of computer instructions that the computer executes to run a program.
17.0 Hash	18.0 An algorithmically generated number that identifies a datum or its location.
19.0 Name space	20.0 A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.

6.0 Revision History

Remote Access:

1.0 Purpose

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

2.0 Scope

This policy applies to all DHHI employees, contractors, vendors and agents with a DHHI owned or personally owned computer or workstation used to connect to the DHHI network. This policy applies to remote access connections used to do work on behalf of DHHI, 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, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

It is the responsibility of DHHI employees, contractors, vendors and agents with remote access privileges to DHHI's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DHHI.

General access to the Internet for recreational use by immediate household members through the DHHI Network on personal computers is permitted for employees that have flat-rate services. The DHHI employee is responsible to ensure the family member does not violate any DHHI policies, does not perform illegal activities, and does not use the access for outside business interests. The DHHI employee bears responsibility for the consequences should the access be misused. Please review the following policies for details

of protecting information when accessing the corporate network via remote access methods, and acceptable use of DHHI's network:

- *Acceptable Encryption Policy*
- *Virtual Private Network (VPN) Policy*
- *Wireless Communications Policy*
- *Acceptable Use Policy*

For additional information regarding DHHI's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

- Secure remote access must be strictly controlled. Control will be enforced via onetime password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
- At no time should any DHHI employee provide their login or email password to anyone, not even family members.
- DHHI employees and contractors with remote access privileges must ensure that their DHHI-owned or personal computer or workstation, which is remotely connected to DHHI'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.
- DHHI employees and contractors with remote access privileges to DHHI's corporate network must not use non-DHHI email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct DHHI business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the DHHI network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
- All hosts that are connected to DHHI internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

- Personal equipment that is used to connect to DHHI's networks must meet the requirements of DHHI-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the DHHI production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

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

5.0 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 1.5 Mbps. Cable
	is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData 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.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
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 DHHI provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into DHHI and an ISP, depending on packet destination.
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).

Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to DHHI's corporate network through a non-DHHI controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-DHHI network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DHHI'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.

6.0 Revision History

Virtual Private Network (VPN) Policy

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the DHHI corporate network.

2.0 Scope
This policy applies to all DHHI employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the DHHI network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

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

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to DHHI internal networks.
- VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by DHHI network operational groups.
- All computers connected to DHHI internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
- VPN users will be automatically disconnected from DHHI's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computers that are not DHHI-owned equipment must configure the equipment to comply with DHHI's VPN and Network policies.
- Only InfoSec-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of DHHI's network, and as such are subject to the same rules and regulations that apply to DHHI-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.

6.0 Revision History

E-mail & Messaging Use and

Retention:

Use:

1.0 Purpose

To prevent tarnishing the public image of DHHI. When email leaves the DHHI domain the general public will tend to view that message as an official policy statement from DHHI.

2.0 Scope

This policy covers appropriate use of any email sent from a DHHI email address and applies to all employees, vendors, and agents operating on behalf of DHHI.

3.0 Policy

3.1 Prohibited Use. The DHHI email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DHHI employee should report the matter to their supervisor immediately.

3.2 Personal Use.

Using a reasonable amount of DHHI resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a DHHI email account is prohibited. Virus or other malware warnings and mass mailings from DHHI shall be approved by DHHI VP Operations before sending. These restrictions also apply to the forwarding of mail received by a DHHI employee.

3.3 Monitoring

DHHI employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. DHHI may monitor messages without prior notice. DHHI is not obliged to monitor email messages.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.

Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to DHHI or its customers' reputation or market standing.
Virus warning	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside DHHI, who do not have a need to know that information.

6.0 Revision History

Retention:

1.0 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 proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope

This email retention policy is secondary to DHHI policy on Freedom of Information and
Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All DHHI email information is categorized into four main classifications with retention guidelines:
Administrative Correspondence (4 years)
Fiscal Correspondence (4 years)

General Correspondence (1 year)
Ephemeral Correspondence (Retain until read, destroy)

3.0 Policy

3.1 Administrative Correspondence

DHHI Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@DHHI has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.2 Fiscal Correspondence

DHHI Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@DHHI has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.3 General Correspondence

DHHI General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence. **3.4 Ephemeral Correspondence**

DHHI Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Instant Messenger Correspondence

DHHI Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

3.6 Encrypted Communications

DHHI encrypted communications should be stored in a manner consistent with DHHI Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.7 Recovering Deleted Email via Backup Media

DHHI maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation, and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

4.0 Enforcement

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

5.0 Definitions

Terms	Definitions
Approved Electronic Mail	Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.
Approved Encrypted email and files	Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within DHHI is done via a license. Please contact the appropriate support organization if you require a license.
Approved Instant Messenger	The Jabber Secure IM Client is the only IM that is approved for use on DHHI 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 UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.
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 DHHI.
Encryption	Secure DHHI 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 your manager and/or corporate legal services for further guidance.

6.0 Revision History

28 July, 2003 Added discussion of backup media

Ethics Policy

1.0 Overview

DHHI purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every DHHI employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

DHHI is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When DHHI addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

DHHI will not tolerate any wrongdoing or impropriety at any time. DHHI will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2.0 Purpose

The purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at DHHI, including all personnel affiliated with third parties.

4.0 Policy

4.1. Executive Commitment to Ethics

Top brass within DHHI must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

Executives must disclose any conflict of interests regard their position within DHHI.

4.2. Employee Commitment to Ethics

DHHI employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

Every employee needs to apply effort and intelligence in maintaining ethics value. Employees must disclose any conflict of interests regard their position within DHHI.

Employees will help DHHI to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

4.3. Company Awareness

Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

DHHI will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

DHHI will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

Employees at DHHI should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

DHHI has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.5. Unethical Behavior

DHHI will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications. DHHI will not tolerate harassment or discrimination.

Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

DHHI will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

DHHI employees will not use corporate assets or business relationships for personal use or gain.

5.0 Enforcement

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

6.0 Definitions

Term	Definition

7.0 Revision History

Firewall

External

Security

1.0 Purpose
This policy establishes information security requirements for all networks and equipment deployed in DHHI located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to DHHI from the damage to public image caused by unauthorized use of DHHI resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope
DHHI networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside DHHI corporate Internet firewalls are considered part of the DMZ and are subject to this policy. This includes DMZ equipment in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to equipment residing inside DHHI's corporate Internet firewalls. Standards for this equipment is defined in the *Internal Security Policy*

3.0 Policy

3.1. Ownership and Responsibilities

1. All new DMZ equipment must accompany a business justification with sign-off at the business unit Vice President level. InfoSec must keep the business justifications on file.
2. Departments are responsible for assigning managers, point of contact (POC), and back up POC, for each department and must maintain up to date POC information with InfoSec [and the corporate enterprise management system, if one exists]. Managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ equipment and establishment of new DMZ equipment connectivity must be requested through a DHHI Network Support Organization and approved by InfoSec.
4. All ISP connections must be maintained by a DHHI Network Support Organization. 5. A Network Support Organization must maintain a firewall device between the DMZ and the Internet.
6. The Network Support Organization and InfoSec reserve the right to interrupt device connections if a security concern exists.
7. The Departments will provide and maintain network devices deployed in the DMZ up to the Network Support Organization point of demarcation.

8. The Network Support Organization must record all DMZ equipment address spaces and current contact information [in the corporate enterprise management system, if one exists].
9. The Department Managers are ultimately responsible for their organizations complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*
11. Individual accounts must be disabled within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
12. InfoSec will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ networks.
2. DMZ equipment must not be connected to DHHI's corporate internal networks, either directly or via a wireless connection.
3. DMZ equipment should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Department Manager must maintain a list of who has access to the equipment.
4. Department Managers are responsible for complying with the following related policies:
    a. *Password Policy*
    b. *Wireless Communications Policy*
    c. **Anti-Virus Policy**
5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the department business needs. All firewall filters will be maintained by InfoSec.
6. The firewall device must be the only access point between the DMZ and the rest of DHHI's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec (including both general configurations and rule sets). InfoSec may require additional security measures as needed.
8. Traffic from the DMZ to the DHHI internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ running Internet Services must be configured to the secure host installation and configuration standards. [Add url link to site where your internal configuration standards are kept].

11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
13. Services and applications not serving business requirements must be disabled.
14. DHHI Confidential information is prohibited on equipment where non-DHHI personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

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

5.0 Definitions

Terms	**Definitions**
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
DMZ (de-militarized zone)	Networking that exists outside of DHHI primary corporate firewalls, but is still under DHHI administrative control.
Network Support Organization	Any InfoSec-approved support organization that manages the networking of non-lab networks.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services .	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc
Network Support Organization Point of Demarcation	The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.

Firewall	A device that controls access between networks, such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.
Internally Connected Lab	A lab within DHHI's corporate firewall and connected to the corporate production network.

6.0 Revision History

Internal Security

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in DHHI located on the internal network. Adherence to these requirements will minimize the potential risk to DHHI from the damage to public image caused by unauthorized use of DHHI resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope

DHHI networks and devices (including but not limited to routers, switches, hosts, etc.) that are Intra-network facing and located inside DHHI corporate Internet firewalls are considered part of the internal network and are subject to this policy. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents.

3.0 Policy

3.1. Ownership and Responsibilities

1. All new equipment must accompany a business justification with sign-off at the business unit Vice President level. InfoSec must keep the business justifications on file.
2. Departments are responsible for assigning managers, point of contact (POC), and back up POC, for each department and must maintain up to date POC information with InfoSec [and the corporate enterprise management system, if one exists]. Managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing network equipment and establishment of new equipment connectivity must be requested through a DHHI Network Support Organization and approved by InfoSec.
4. A Network Support Organization must maintain a firewall device between the production environment and the DMZ.
5. The Network Support Organization and InfoSec reserve the right to interrupt device connections if a security concern exists.

6. The IS/IT/InfoSec staff will provide and maintain network devices deployed in the network up to the Network Support Organization point of demarcation.
7. The IS/IT/InfoSec staff must record all equipment address spaces and current contact information [in the corporate enterprise management system, if one exists].
8. The Department Managers are ultimately responsible for their organizations complying with this policy.
9. Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*
10. Individual accounts must be disabled within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
11. InfoSec will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources outside of the corporate network.
2. DHHI's corporate internal networks may not be accessed, either directly or via a wireless connection, by resources or devices outside of the production environment.
3. Network equipment should be in a physically separate room from any DMZ connected devices. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Department Manager must maintain a list of who has access to the equipment.
4. Department Managers are responsible for complying with the following related policies:
    a. *Password Policy*
    b. *Wireless Communications Policy*
    c. **Anti-Virus Policy**
5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the department business needs. All firewall filters will be maintained by InfoSec.
6. The firewall device must be the only access point between the DMZ and the rest of DHHI's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec (including both general configurations and rule sets). InfoSec may require additional security measures as needed.
8. Access to resources on DHHI’s network will be granted based on Extended Access Control Lists(Extended ACLs) which will utilize a most restrictive logic combining source & destination IP addressing, and protocol level filtering.

9. InfoSec staff will be responsible to configuring and updating Extended ACLs on DHHI's internal firewall equipment connected to production level resources.
10. All routers and switches not used for testing and/or training must conform to the Network Router and Switch standardization documents.
11. Current applicable security patches/hot-fixes for any applications must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
13. Services and applications not serving business requirements must be disabled.
14. DHHI Confidential information is prohibited on equipment where non-DHHI personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

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

5.0 Definitions

Terms	**Definitions**
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
Extended ACL	Lists kept by routers to control access to or from the router for a number of services. These access lists specifically filter packets based on source & destination IP address as well as applicable protocol and are usually applied closest to the source of the packet, for most effective filtering (for example, to prevent packets with a certain IP address from leaving a particular interface on the router destined for a specific address using a specific protocol like telnet; port 23).

DMZ (de-militarized zone)	Networking that exists outside of DHHI primary corporate firewalls, but is still under DHHI administrative control.
Network Support Organization	Any InfoSec-approved support organization that manages the networking of non-lab networks.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services .	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc
Network Support Organization Point of Demarcation	The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or firewall.
Firewall	A device that controls access between networks, such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.
Internally Connected Lab	A lab within DHHI's corporate firewall and connected to the corporate production network.

6.0 Revision History

IDS

1.0 Purpose

The purpose of this policy is to provide guidelines for Intrusion Detection systems as implemented within the DHHI network both within the network infrastructure and on the perimeter of the network.

2.0 Scope

This policy applies to all DHHI InfoSec employees

3.0 Policy

3.1 Guidelines

There must be a minimum of two network based Intrusion Detection Systems running at all times on DHHI's network, both should be located at the perimeter of the network, at the firewall bordering the DMZ. The IDS signatures must be updated every 2 weeks from the vendor to keep the IDS(s) at current signature level. Any suspected intrusions, suspicious activity, or unexplained erratic system behavior discovered by administrators, users, or computer security personnel

must be reported to the organizational IT computer security office within 1 hour and the Incident Response plan should be initiated. All intrusions with financial or customer data loss must be reported to CEO, CFO, CIO within 7 days of the loss.

Refer to the DHHI Incident Response Policy Manual for further details regarding events.

3.2 Logging

The IDS logs must be kept for minimum of 1 year. The IDS Event logs must be monitored daily by InfoSec Staff for abnormal activities.

3.3 Ownership

Responsibility for maintenance, including signature updates, firmware updates and system testing, as well as any future iterations of IDS implementations, will fall to the InfoSec team with ultimate approval from the CISO and InfoSec manager.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Intrusion Detection System (IDS)	Used to detect several types of malicious behaviors that can compromise the security and trust of a computer system.

6.0 Revision History

Systems Management

1.0 Purpose

The purpose of this policy is to provide guidelines for system management as implemented within the DHHI network both within the network infrastructure, pertaining to workstations and server class computers.

2.0 Scope

This policy applies to all DHHI IS/IT employees

3.0 Policy

3.1 Guidelines

Basic Client Computer Configuration Policy

All computer systems must be configured according to the NIST checklist to ensure patching against the common system vulnerabilities. All systems must receive Operating System updates from the local Software Update Server, as

dictated by the development team so as to ensure continued functionality of company proprietary software packages.

Basic Server Computer Configuration Policy

All servers must be hardened against common system vulnerabilities using the NIST Guides and vendor security update announcements. The server infrastructure will receive updates via SUS to ensure thorough and consistent system configurations. There must be minimum level of security controls installed on each server to protect the infrastructure. All servers changes, updates, upgrades must be approved through the change proposal process and logged into a change management database with timestamps.

4.0 Enforcement

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

5.0 Definitions

Term	Definition

6.0 Revision History

Planning

Diamond Hands Holding Inc

Incidence Response/ Disaster Recovery Manual

Table of Contents

Contingency Planning:

1.0 Purpose

The purpose of this policy is to provide the basis of appropriate response to incidents or disasters that threaten the confidentiality, integrity, and availability of Diamond Hands Holdings Inc. information assets, information systems, and the networks that deliver the information. This policy has been developed to provide guidance for response to and address potential incidents and disasters as they may occur against DHHI.

2.0 Scope

This policy applies to all employees at DHHI, all systems and all services that the IS/IT/InfoSec staff is responsible for. This document serves as a guideline for deployment of trained Security Incident Response Teams in a crisis situation dealing with potential incidents and disasters as listed herein but is not limited to only those events as published.

3.0 Contingency Planning Committee

3.1. Responsibilities

The Incident Response Planning Committee is a representative collection of individuals with a stake in the successful and uninterrupted operation of DHHI. The Incident Response Planning Committee is charged with the development, testing, and maintenance the Incident Response Plan.

3.2. Members

The following DHHI employees are members of the Contingency Planning Committee.

- **Jake Bulim (CEO)**

4.0 Definition of Critical Incidents

A critical incident is any adverse event, man-made or force of nature (see Table 1), which threatens the confidentiality, integrity, or availability of DHHI information systems and network infrastructure.

Category	Characteristic
Acts of Human Error or Failure	• **Accidental deletion of user desktop data or files by personnel (accidental user data deletion)** • **Improper configuration of software or hardware**
Compromises to Intellectual Property	• **Unauthorized installation of software in violation of its licensing (piracy)** • **Release of organizational information performed outside the bounds of policy, sometimes classified as a "leak"** • **Violation of fair use of copyrighted material (plagiarism)**
Deviations in Quality of Service by Service Providers	• **Network connection outage due to cable severance (phone or ISP)**

Category	Characteristic
Technical Hardware Failures or Errors	• **Equipment failure due to manufacturer or designer faults or defects.**
Technical Software Failures or Errors	• **Software failure due to manufacturer or designer faults or defects (for example, bugs or code problems)** • **Unknown software access bypasses (loopholes and trapdoors)**
Technological Obsolescence	• **Use of antiquated or outdated technologies** • **Failure to maintain or update antiquated or outdated equipment-based data storage**

Table 1 Threats (potential incidents) adopted from the Whitman ACM Model

Based on the nature and severity of the incident or disaster the following policies will be implemented and the appropriate teams will be notified.

- *Incident Response Plan (page 7 of this document)*
- *Disaster Recovery Plan(page10 of this document)*

5.0 Organizations Structure & Delineation of Roles, Responsibilities & Levels of Authority:

5.1. Cyber Triage and Forensic

The Cyber Triage and Forensic (CTF) will consist of information technology staff and managers from all departments within DHHI. The CTF implements the policies and procedures, according to the Incident Response or Disaster Recovery Plans, in the event of an incident, as defined by either the IRP or DRP.

5.2. Incident Response and Contingency Coordinator

The Critical Incident Coordinator is designated by the DHHI management team, either the InfoSec Manager for IS incidents or VP of Operations for a natural disasters, to act as the lead in the event a critical incident occurs. This individual is response for the management and process of the incident and the incident response or disaster recovery plan.

5.3. Digital Forensics Incident Response (DFIR)

The Digital Forensics Incident Response (DFIR) consists of fulltime employees with information technology job functions who have been specially trained in IS incident management, each member has a distinct response role. The DFIR works under the direction of the InfoSec Manager.

5.3.1. Responsibilities

The DFIR main focus is to implement the IRP when a critical IS incident occurs, that is higher than a category one incident according to the IRP. In the event of such a critical incident, normal job functions are considered secondary until the incident is resolved.

5.3.2. Members

- InfoSec Manager

5.4. Users

Users are DHHI employees that are not directly involved in the incident response process however, play a major role as a notification mechanism. Their responsibility is to inform the information technology staff that a potential incident has occurred.

5.5. Categorization Of Incidents

Each incident can be assigned a category rating See Section 4.2 of the IRP (page 6 of this document)

5.6. Performance Measures

Performance will be judged on response time and recovery time based on the Categorization of the incident.

5.7. Documentation

For each incident that occurs, a series of documents will be filled out and kept for a period of one year.

5.7.1. Incident Forms

The following is a list of forms required for each incident; see section 5 of IRP for definitions (page 8 of this document)

- Incident declaration
- Incident status update
- Incident closure and end of recovery
- Incident Review
- Incident Response Plan Addendum to Attack Success End Case

5.7.2. Contact List

The following documents are maintained in Appendix A of this document (page 12 of this document)

- Notification List
- First Responders List
- Emergency Contact List

Incident Response

1.0 Purpose

The purpose of this incident response plan is to provide general guidance to both the technical and managerial staff of the Information Security department at DHHI. This plan will enable, quick and efficient response to and recovery from incidents, and enable qualified staff to carry out all necessary steps to correctly handle an incident, prevent or minimize disruption of critical computing services, and minimize impact on information systems owned by or in the control of DHHI.

This document also serves as a guide for sharing information with other organizations both internally and externally including other information security and law enforcement agencies, as well as a guide for pursuing appropriate legal action.

2.0 Scope

The guidance contained in this document is applicable to the Information Security staff at DHHI. but emphasis is placed on the CTF . This plan is to be implemented in the event an incident occurs, closed when the incident is declared to be resolved by an appropriate DHHI. official.

3.0 Roles & Responsibilities

Each Employee member has responsibilities related to the security of all DHHI. computing systems and networks. Due to this stipulation, non-critical incidents will be handled by DHHI system administrators in the department in which the incident occurs. In the event that an incident is identified as critical and an SIRT assembly is mandated, then the CTF will take control of the incident until it is resolved. Employees play a major role in this process as they function as the initial notification mechanism by detecting the event and then notifying the IS team.

4.0 Procedure:

4.1. If an employee discovers an incident, they will immediately notify the DHHI Help Desk by phone and a trouble ticket will be opened and escalated to the InfoSec department.

Information collected by the help desk will consist of

- What was found
- The time of the discovery
- A description of the incident
- Names of all employees involved.

4.2. A senior technician will review the ticket and place the incident into a category. Any incident rated two; three or four is escalated immediately to the InfoSec team by phone and email. The categories are as follows:

- Category one – A disruption in service. Small attacks.
- Category two – Possible or actual downtime to customer servers or low priority servers.
- Category three – Possible or actual downtime to any core servers or network equipment.
- Category four – Complete loss of service.

4.3. Members in the InfoSec department will review the ticket and investigate the incident, forming the CTF if necessary.

4.4. After the incident has been properly identified, members will follow the appropriate procedure given for the situation. Members can create procedures other than the following at any time to improve the quality of this document. Current procedures include:

- Power spike or brown-out procedure
- DDOS attacks procedure
- Active attack procedure

4.5. CTF will isolate the affected systems

4.5.1. If the system is mission critical CTF will make every effort to minimize system downtime. The system will be bit-copied and returned to service as soon as the incident is contained and the system is deemed safe by CTF.

4.5.2. If the system is determined to be non mission critical, it will be taken out of service and bit copied for forensic investigation, returning to service only after the investigation is concluded.

4.6. CTF will investigate to determine how the incident was caused. Once determined, system/network vulnerabilities will be resolved, operational change recommendations will be submitted to managers and the network administrator for approval. Upon approval, they will be implemented and the IRP will be modified as necessary.

A file will be created with documentation for each incident. The following documents will be required:

5.0 Forms

There are several forms to be utilized throughout the IR process they are:

Form	Use
• Incident declaration	**Used to specify the details of the incident once determined critical by IS staff.**
• Incident status update	**Used to notify C-level and managerial staff disposition of incident during the course of the investigation.**
• Incident closure and end of recovery	**Used at the end of an investigation to officially disposition the case as "closed" and determine if the affected systems can be returned to service.**
• Incident Review	**Used at the end of the investigation to determine what process flows could be modified for efficiency and determine if legal recourse is necessary.**

Form	Use
• Incident Response Plan Addendum to Attack Success End Case	**Used to modify the IR plan according to investigation findings to prevent future occurrences.**

Templates can be found in Appendix B (page 14 of this document)

6.0 Planning, Testing, Training, & Exercises

This plan is to be tested bi-annually. Training and exercises for this plan will be conducted quarterly.

Appropriate testing, training, and exercises are to be decided by DHHI. officials and are non-negotiable. Testing, training and exercises should be achievable and should not interfere with everyday business, or at least should conflict at a minimum.

7.0 Review Schedule

The Information Security department at DHHI., along with the CTF, will review this plan on an annual basis and at case closing of an incident and made changes accordingly if they are required. If a change to this plan is made, affected parties will be notified.

Disaster Recovery:

1.0 Purpose

The purpose of this policy is to provide a plan to respond to a disaster that destroys or severely cripples the Facility's central computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

2.0 Objectives

This disaster recovery plan has the following primary objectives:

1) Present an orderly course of action for restoring critical computing capability to the DHHI. facility within 14 days of initiation of the plan.
2) Set criteria for making the decision to recover at a cold site or repair the affected site.
3) Describe an organizational structure for carrying out the plan.
4) Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5) Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

2.0 Notification

An Automated Emergency Notification System is required by policy. The system should call employees in order of Chain of Command to notify special teams, officials, and other employees if and where to report.

3.0 Recovery Facility

If DHHI. facility is destroyed in a disaster, repair or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at an alternate site.

The Facility has a number of options for alternate sites. The options are not limited to but include:

- Hot Site

- Cold Site
- Relocation to other municipal facilities outside of the affected area.

4.0 Safety Issues

All disaster recovery procedures should be performed in conjunction with local authorities to ensure safety in all areas. In cases where officials deem it unsafe to continue or perform an action, that asset maybe classified as a loss.

5.0 Data Protection Strategies

In preparation for a disaster, the InfoSec Manager will continue standard data backup strategies from the on-site RAID array. Specifically: Monday through Thursday onsite differential backups. Friday full backups are stored off-site at a location to be determined by the InfoSec Manager. DHHI. will also implement remote backup for critical data using Iron Mountain as a primary site and Nighthawk as a secondary provider.

In the event of a disaster only authorized personnel will be allowed on site for security and safety reasons. Data recovery should be considered a sensitive matter and will be handled exclusively by a data recovery team.

6.0 Disaster Recovery Teams

Employees will be trained and assigned to Disaster Recovery Teams. Examples of such teams are not limited to but include the following:

- Recovery Management Team
- Damage Assessment Team

7.0 Equipment Protection & Salvage

Below is information on procedures to be used immediately following a disaster to preserve and protect resources in the affected area.

It is imperative that any equipment, magnetic media, paper stocks, and other items at the damaged primary site be protected from the elements to avoid any further damage so and attempt can be made to recover data.

- Gather all magnetic tape cartridges into a central area and quickly secure them in antistatic, non-metal containers, to avoid water damage.
- Cover all computer equipment to avoid water damage.
- Cover all undamaged paper stock to avoid water damage.
- Ask local authorities to post security guards at the primary site to prevent property theft or vandalism.

After securing the media and equipment a line-item inventory should be conducted and all assets catalogued. Once completed, a secure recovery site should be established, equipment should be transported and data recovery should begin as soon as possible to avoid further loss.

8.0 Damage Assessment

The initial damage assessment is performed to determine the extent of damage to company assets and housing facilities. Once the extent of damage is assessed, a priority is assigned to “lost” equipment and management is notified.

9.0 Equipment & Supplies

Each department must submit a list of equipment and supplies needed to continue normal business operations. These lists, as well as vendor contact information, should be stored with the DRP manual

10.0 Planning, Testing, Training & Exercises

This plan is to be tested bi-annually. Training and exercises for this plan will be conducted quarterly, to include simulated data loss, fire, flood, electrical outage, and tornado/hurricane (depending on site location).

Appropriate testing, training, and exercises are to be decided by DHHI. officials and are non-negotiable. Testing, training and exercises should be achievable and should not interfere with everyday business, or at least should conflict at a minimum.

11.0 Review Schedule

The InfoSec Office at DHHI. will review this plan on an annual basis and make necessary changes. If a change to this policy is made, affected parties will be notified.

Appendix A (Contact Lists)

Notification List

Name:	Title	Role	Cell Phone:	Home Phone:

First Responders List

Name:	Title	Role	Cell Phone:	Home Phone:

Emergency Contact List

Name:	Title	Role	Cell Phone:	Home Phone:

Appendix B (Form Templates)

Incident Declaration

Case Number: Status:
Reported By: 1st Responder:
Case Manager:
Date: Time:
Attack Type:
Trigger:
Reaction Force and Lead:
Notification Method:
Response Time:
Incident Occurrence Procedures
1.
Post Incident Procedures
1.
Incident Preparation Procedures
1.

Incident Status Update:

Date: Time:
To:
From:
Issue/ Incident:
Affected Systems
1)
Impact on DHHI Assets:
1)
Action Plan:

Next Available Update: Date/Time
Signature:

Incident Closure & End of Recovery
Case Number: Status:
Case Manager:
Date: Time:
Nature of incident:

Affected system(s)
1)
Resolution Steps:
1)

Was Data Lost? Y / N Financial Impact: $
Was System Equipment Recovered? Y / N Returned to service? Y / N
Notes:

Is the incident completely resolved /case closed? Y / N
Configuration Changes

Network Infrastructure Changes

Signature:

Incident Review:

Case Number: **Status:**
Case Manager:
Date: **Time:**
Nature of incident:
Is Legal Recourse Required? **Y / N**
Based on incident cause and steps to resolution, are there any processes or procedures that could be modified to
1) **Prevent the issue from reoccurring**
Notes:

2) **Make detection resolution more efficient**
Notes:

Signature:

Incident Response Plan Addendum to Attack Success End Case

Case Number: Status:
Case Manager:
Date: Time:
Nature of incident:

Planned Policy Changes:
1)
Policy: Section:
Change Impact:

Effective Date:
InfoSec Manager Signature & Date:

Change Control Manager Signature & Date:

VP Operations Signature & Date:

Attach Signed New Policy and Insert in Appropriate Policy Document
Sign When Completed:

Statement of Risk for Current Investors

Risk Factors

There are many factors that affect DHHI's business and the results of its operations, some of which are beyond DHHI's control. The following is a description of some of the important factors that may cause the actual results of DHHI' operations in future periods to differ materially from those currently expected or desired.

Rapidly Evolving Market

We operate in a rapidly evolving market and must, among other things:

- Respond to competitive developments.
- Continue to upgrade and expand our product and services offerings.
- Continue to attract, retain and motivate our employees.

Fluctuating Operating Results

We cannot predict our future revenues and operating results with certainty. However, we do expect our future revenues and operating results to fluctuate due to a combination of factors, including:

- The extent to which the public perceives that unauthorized access to and use of online information are threats to network security.
- Customer budgets
- The mix of product sales among the various products offered by DHHI and whether revenue is recognized upon sale or deferred to subsequent periods.
- The volume and timing of orders, including seasonal trends in customer purchasing.
- Our ability to develop and timely introduce new and enhanced product and managed service offerings.
- The introduction and acceptance rate of new DHHI branded appliances, including related increased cost of goods sold.
- Our ability to accurately forecast and produce demanded quantities of our appliance products and models.
- Availability of component parts of appliance products and reliance on contract manufacturers to produce such products.
- Our ability to provide scalable managed services offerings in a cost effective manner.
- Foreign currency exchange rates that affect our international operations.
- Whether enterprises consolidate their security platforms with fewer vendors and whether DHHI benefits from this.
- Product and price competition in our markets.
- General economic conditions, both domestically and in our foreign markets.

We focus our direct sales efforts on enterprise-wide security solutions, which consist of our entire product suite, professional services, and managed security services, rather than on the sale of component products. As a result, each sale requires substantial time and effort from our sales and support staff. In addition, the revenues associated with particular sales vary significantly depending on the number of products acquired by a customer and the number of devices used by the customer.

Large individual sales, or even small delays in customer orders, can cause significant variation in our license revenues and results of operations for a particular period. The timing of large orders is usually difficult to predict and, like many software-based technology companies, many of our customers typically complete transactions in the last month of a quarter.

We cannot predict our operating expenses based on our past results. Instead, we establish our spending levels based in large part on our expected future revenues. As a result, if our actual revenues in any future period fall below our expectations, our operating results likely will be adversely affected because very few of our expenses vary with our revenues. We believe that our quarterly and annual revenues, expenses and operating results likely will vary significantly in the future.

Our ability to provide timely guidance and meet the expectations of investors with respect to our operating and financial results is affected by the tendency of a majority of our product and license sales to be completed in the last month of a quarter. We may not be able to determine whether we will experience material deviations from guidance or expectations until the end of a quarter.

Third Party Supplier and Manufacturer Dependence

Little inventory of our appliance products is carried and we rely on suppliers to deliver necessary components to our contract manufacturers in a timely manner based on the forecasts we provide. If shortages occur, supplies are interrupted, or we underestimate demand for models, we may not be able to deliver products to our customers and our revenue would be adversely affected.

Forecasts of our demand to our contract manufacturers are provided. Because our supply of hardware is based on short-term forecasts and purchase orders, our contract manufacturers are not obligated to purchase components for greater quantities over longer periods. If we underestimate our requirements, our contract manufacturers may have an inadequate component inventory and, based on lead times, this could interrupt manufacturing and result in delays in shipments and revenues.

Market Competition

The market for network security monitoring, detection, prevention and response solutions is intensely competitive, and we expect competition to increase in the future. We cannot guarantee that we will compete successfully against our current or potential competitors, especially those with significantly greater financial resources or brand name recognition. Our chief competitors generally fall within the following categories:

- Large companies that sell competitive products and offerings, as well as other large software companies that have the technical capability and resources to develop competitive products.
- Software or hardware network infrastructure companies that could integrate features that are similar to our products into their own products.
- Smaller software companies offering relatively limited applications for network and Internet security.
- Small and large companies with competitive offerings to components of our managed service offerings.

Mergers or consolidations among these competitors, or acquisitions of small competitors by larger companies, represent risks. These acquisitions will make these entities potentially more formidable competitors to us if such products and offerings are effectively integrated. Large companies may have advantages over us because of their longer operating histories, greater name recognition, larger customer bases or greater financial, technical and marketing resources.

As a result, they may be able to adapt more quickly to new or emerging technologies and changes in customer requirements. They can also devote greater resources to the promotion and sale of their products than we can. In addition, these companies have reduced the price of their security monitoring, detection, prevention and response products and managed security services, which increases pricing pressures within our market.

Several companies currently sell software products (such as encryption, firewall, operating system security and virus detection software) that our customers and potential customers have broadly adopted. Some of these companies sell products that perform the same functions as some of our products. In addition, the vendors of operating system software or networking hardware may enhance their products to include the same kinds of functions that our products currently provide.

The widespread inclusion of comparable features to our software in operating system software or networking hardware could render our products less competitive or obsolete, particularly if such features are of a high quality. Even if security functions integrated into operating system software or networking hardware are more limited than those of our products, a significant number of customers may accept more limited functionality to avoid purchasing additional products.

In addition, we have offerings that compete with vendors of firewalls, VPNs, anti-virus systems, and content/spam filtering products. These offerings are competitive with a broader spectrum of network security companies, as well as those that also offer integrated security appliances or broad product suites.

Risks Associated with Governmental Contracting

Our customers include the U.S. and other national government agencies and a significant number of other state and local governments or agencies.

- **Procurement**—Contracting with public sector customers is highly competitive

and can be expensive and time-consuming, often requiring that we incur significant upfront time and expense without any assurance that we will win a contract;

- **Budgetary Constraints and Cycles**—Demand and payment for our products and services are impacted by public sector budgetary cycles and funding availability, with funding reductions or delays adversely impacting public sector demand for our products and services;
- **Modification or Cancellation of Contracts**—Public sector customers often have contractual or other legal rights to terminate current contracts for convenience or due to a default. If a contract is canceled for convenience, which can occur if the customer's product needs change, we may only be able to collect for products and services delivered prior to termination. If a contract is canceled because of default, we may only be able to collect for products and alternative products and services;
- **Governmental Audits**—National governments and other state and local agencies routinely investigate and audit government contractors' administrative processes. They may audit our performance and pricing and review our compliance with applicable rules and regulations. If they find that we improperly allocated costs, they may require us to refund those costs or may refuse to pay us for outstanding balances related to the improper allocation. An unfavorable audit could result in a reduction of revenue, and may result in civil or criminal liability if the audit uncovers improper or illegal activities.

Rapid Technological Change and Frequent Introduction of New Product

Rapid changes in technology pose significant risks to us. We do not control nor can we influence the forces behind these changes, which include:

- The extent to which businesses and others seek to establish more secure networks.
- The extent to which hackers and others seek to compromise secure systems.
- Evolving computer hardware and software standards.
- Changing customer requirements.
- Frequent introductions of new products and product enhancements.

To remain successful, we must continue to change, adapt and improve our products in response to these and other changes in technology. Our future success hinges on our ability to both continue to enhance our current line of products and professional services and to introduce new products and services that address and respond to innovations in computer hacking, computer technology and customer requirements.

We cannot be sure that we will successfully develop and market new products that do this. Any failure by us to timely develop and introduce new products, to enhance our current products or to expand our professional services capabilities in response to these changes could adversely affect our business, operating results and financial condition.

Our products involve very complex technology and, as a consequence, major new

products and product enhancements require a long time to develop and test before going to market. Because this amount of time is difficult to estimate, we have had to delay the scheduled introduction of new and enhanced products in the past and may have to delay the introduction of new and enhanced products in the future.

The techniques computer hackers use to gain unauthorized access to, or to sabotage, networks and intranets are constantly evolving and increasingly sophisticated. Furthermore, because new hacking techniques are usually not recognized until used against one or more targets, we are unable to anticipate most new hacking techniques. To the extent that new hacking techniques harm our customers' computer systems or businesses, affected or prospective customers may believe that our products are ineffective, which may cause them or prospective customers to reduce or avoid purchases of our products.

Undetected Product Error or Defect

We offer warranties on our products, allowing the end customer to have any defective product repaired, or to receive a replacement product for it during the warranty period, or in certain circumstances return the product for a refund. Our products may contain undetected errors or defects. If there is a broad product failure across our customer base, we may decide to replace all affected products or we may decide to refund the purchase price for defective units. Such defects and actions may adversely affect our ability to record revenue. Some errors are discovered only after a product has been installed and used by end customers. Any errors discovered after commercial release could result in loss of revenues and claims against us.

We offer warranties on our service levels for managed security services. If we do not meet warranties, the customer generally may obtain credits for service. If we are unable to fix errors or other product problems that later are identified after full deployment, or if we fail to meet our service levels for managed security services, in addition to the consequences described above, we could experience:

- Failure to achieve market acceptance.
- Loss of customers.
- Loss of or delay in revenues and loss of market share.
- Diversion of development resources.
- Increased service and warranty costs.
- Legal actions by our customers.
- Increased insurance costs.

Product Complexity

Because we offer very complex products, undetected errors, failures or bugs may occur when they are first introduced or when new versions are released. Our products often are installed and used in large-scale computing environments with different operating systems, system management software and equipment/networking

configurations. This variance of offerings may expose undetected errors, failures or bugs in our products.

Our customers' computer environments are often characterized by a wide variety of standard and non-standard configurations that make pre-release testing for programming or compatibility errors very difficult and time- consuming. Despite testing, errors, failures or bugs may not be found in new products or releases until after commencement of commercial shipments. Errors, failures or bugs in products released by us could result in negative publicity, product returns, loss of or delay in market acceptance of our products or claims by customers or others.

In addition, if an actual or perceived breach of network security occurs in one of our end customer's security systems, regardless of whether the breach is attributable to our products, the market perception of the effectiveness of our products could be harmed. Because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, we may be unable to anticipate these techniques. Alleviating any of these problems could require significant expenditures of our capital and resources and could cause interruptions, delays or cessation of our product licensing, which could cause us to lose existing or potential customers and would adversely affect results of operations.

Lawsuits or Damages in Connection With Any Alleged or Actual Failure of Our Products and Services

Because our products and services provide and monitor network security and may protect valuable information, we could face claims for product liability, tort or breach of warranty. Anyone who circumvents our security measures could misappropriate the confidential information or other property of end customers using our products, or interrupt their operations. If that happens, affected end customers or others may sue us. In addition, we may face liability for breaches caused by faulty installation of our products by our service and support organizations.

Provisions in our contracts relating to warranty disclaimers and liability limitations may be unenforceable. Some courts, for example, have found contractual limitations of liability in standard computer and software contracts to be unenforceable in some circumstances. Defending a lawsuit, regardless of its merit, could be costly and could divert management attention. Our business liability insurance coverage may be inadequate or future coverage may be unavailable on acceptable terms or at all.

Global Operations

The expansion of our international operations includes our presence in dispersed locations throughout the world, including throughout EMEA and the Asia/Pacific and Latin America regions. Our international presence and expansion exposes us to risks not present in our U.S. operations, such as:

- The difficulty in managing an organization spread over various countries located across the world.

- Compliance with, and unexpected changes in, a wide range of complex regulatory requirements in countries where we do business.
- Duties and tariffs imposed on importation of our products in other jurisdictions where other manufacturers may not bear those same costs.
- Increased financial accounting and reporting burdens.
- Potentially adverse tax consequences.
- Fluctuations in foreign currency exchange rates resulting in losses or gains from transactions and expenses denominated in foreign currencies.
- Reduced protection for intellectual property rights in some countries.
- Reduced protection for enforcement of creditor and contractual rights in some countries.
- Import and export license requirements and restrictions on the import and export of certain technology, especially encryption technology and trade restrictions.

Despite these risks, we believe that we must continue to expand our operations in international markets to support our growth. To this end, we intend to establish additional foreign sales operations, expand our existing offices, hire additional personnel, expand our international sales channels and customize our products for local markets. If we fail to execute this strategy, our international sales growth will be limited.

Networks, Products and Services May be Targeted by Hackers

Like other companies, our websites, networks, information systems, products and services may be targets for sabotage, disruption or misappropriation by hackers. As a leading network security solutions company, we are a high profile target. Although we believe we have sufficient controls in place to prevent disruption and misappropriation, and to respond to such situations, we expect these efforts by hackers to continue. If these efforts are successful, our operations, reputation and sales could be adversely affected.

Necessity of Successfully Integrated Acquisitions

As part of our growth strategy, we have and may continue to acquire or make investments in companies with products, technologies or professional services capabilities complementary to our solutions. When engaging in acquisitions, we could encounter difficulties in assimilating or completing the development of the technologies, new personnel and operations into our company. These difficulties may disrupt our ongoing business, distract our management and employees, increase our expenses and adversely affect our results of operations. These difficulties could also include accounting requirements, such as impairment charges related to goodwill or other intangible assets.

We cannot be certain that we will successfully overcome these risks with respect to any future acquisitions or that we will not encounter other problems in connection with our

recent or any future acquisitions. In addition, any future acquisitions may require us to incur debt or issue equity securities. The issuance of equity securities could dilute the investment of our existing stockholders.

Cash Shortage

In July 2005, DHHI announced a share repurchase program authorizing the use of up to $100 million in cash to repurchase outstanding shares of our common stock. We expect to repurchase shares for cash as business conditions warrant through July 19, 2006. The full implementation of this repurchase program would use a significant portion of our cash reserves. This use of cash could limit our future flexibility to complete acquisitions of businesses or technology or other transactions.

Proprietary Rights May be Difficult to Enforce

We rely primarily on copyright, trademark, patent and trade secrets laws, confidentiality procedures and contractual provisions to protect our proprietary rights. We hold several United States patents, one Taiwanese patent, and have a number of patent applications pending. We also hold numerous United States and foreign trademarks and have a number of trademark applications pending. There can be no assurance that patents will be issued from pending applications, or that claims allowed on any patents will be sufficiently broad to protect our technology.

There can be no assurance that any issued patents will not be challenged, invalidated or circumvented, or that any rights granted under these patents will actually provide competitive advantages to us. Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our products or to obtain and use information that we regard as proprietary.

Policing unauthorized use of our products is difficult. While we cannot determine the extent to which piracy of our software products occurs, we expect software piracy to be a persistent problem. In addition, the laws of some foreign countries do not protect our proprietary rights to as great an extent as do the laws of the United States, and many foreign countries do not enforce these laws as diligently as U.S. government agencies and private parties.

If we are unable to protect our proprietary rights to the totality of the features in our software and products (including aspects of our software and products protected other than by patent rights), we may find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create the innovative products that have enabled us to be successful.

Proprietary Right Infringement of Others

Third parties may assert claims or initiate litigation related to exclusive patent, copyright, trademark and other intellectual property rights to technologies that are relevant to our business. Because of the large number of patents in the Internet, networking, security and software fields, the secrecy of some pending patents and the rapid rate of issuance of new patents, it is not economically practical (or even possible) to determine in

advance whether a product (or any of its components) infringe or will infringe the patent rights of others.

Third party asserted claims and/or initiated litigation can include claims against us or our manufacturers, suppliers, or customers, alleging infringement of proprietary rights with respect to our existing or future products (or components of those products). Regardless of the merit of these claims, they can be time-consuming, result in costly litigation and diversion of technical and management personnel; or require us to develop a non-infringing technology and enter into license agreements.

There can be no assurance that licenses will be available on acceptable terms and conditions, if at all, in these circumstances, or that any indemnification that might be available to us would be adequate to cover our costs of defense. Furthermore, because of the potential for large judgments, which are not necessarily predictable, it is not unusual to find even arguably felonious claims settled for significant funds.

If any infringement or other intellectual property claims made against us by a third party is successful, or if we fail to develop non-infringing technology or license the proprietary rights on commercially reasonable terms and conditions, our business, operating results, financial condition and liquidity could be materially and adversely affected.

References:

Whitman, M & Mattord, H. (2004) Management of Information Security, Boston: Course Technology.

Whitman, M. & Mattord, H. (2007) Principals of Incident Response and Disaster Recovery. Boston: Course Technology.

All issue-specific policies modified from The SANS Institute, Information Security Policies < http://www.sans.org/resources/policies/>