# DHI

# Information Security Policy

**Registered to:**

**The State of Washington Administrative Office of the Courts**

**Version 1.11**

**October 2014**

**BY ITS ACCEPTANCE OF THIS COPY OF INFORMATION SECURITY POLICIES AND PROCEDURES, AND IN ACCORDANCE THE NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT SIGNED BY THE RECIPIENT, THE RECIPIENT AGREES THAT (A) IT WILL NOT, IN WHOLE OR IN PART, AT ANY TIME, DISTRIBUTE INFORMATION SECURITY POLICY AND PROCEDURES TO OTHERS OR REPRODUCE IT WITHOUT THE PRIOR WRITTEN CONSENT OF THE COMPANY AND (B) IT WILL KEEP PERMANENTLY CONFIDENTIAL ALL INFORMATION CONTAINED HEREIN OR MADE AVAILABLE IN CONNECTION WITH ANY FURTHER INVESTIGATION. INFORMATION SECURITY POLICIES AND PROCEDURES IS BEING DELIVERED FOR INFORMATIONAL PURPOSES. UPON REQUEST, THE RECIPIENT WILL PROMPTLY RETURN ALL MATERIAL RECEIVED FROM THE COMPANY (INCLUDING THIS NUMBERED INFORMATION SECURITY POLICIES AND PROCEDURES DOCUMENT) WITHOUT RETAINING ANY COPIES THEREOF. IN FURNISHING THIS INFORMATION SECURITY POLICIES AND PROCEDURES, THE COMPANY UNDERTAKES NO OBLIGATION TO PROVIDE THE RECIPIENT WITH ACCESS TO ANY ADDITIONAL INFORMATION OR TO UPDATE ANY OF THE INFORMATION CONTAINED HEREIN.**

Drivers History Inc
1 Keystone Ave
Unit 700
Cherry Hill, New Jersey 08003
P:800-974-8422

*The information contained herein is confidential and proprietary to DHI.*
*Unauthorized disclosure is prohibited.*

# Table of Contents


1. INFOSEC Policy ..... 3
2. Acceptable Encryption Policy ..... 6
3. Acceptable Use Policy ..... 7
4. Access Recertification Policy ..... 11
5. Acquisition Assessment Policy ..... 12
6. Anti-Virus and Malware Policy ..... 14
7. Audit Policy ..... 16
8. Audit Logs Retention Policy ..... 17
9. Automatically Forwarded Email Policy ..... 18
10. Bluetooth Communication Policy ..... 19
11. Change Management Policy ..... 20
12. Contractor Access Policy ..... 29
13. Data Security Policy ..... 34
14. Data Recovery Policy ..... 35
15. Employee Education Policy ..... 37
16. Encryption Standards Policy ..... 38
17. Extranet Policy ..... 39
18. Firewall Policy ..... 41
19. General Host Configuration Standards Policy ..... 45
20. Incident Reporting Policy ..... 46
21. Information Sensitivity Policy ..... 47
22. Internal Lab Security Policy ..... 54
23. Internet DMZ Equipment Policy ..... 58
24. Laptop Security Policy ..... 61
25. Mass Storage Device Policy ..... 62
26. Media and Data Destruction Policy ..... 63
27. Password Policy ..... 65
28. Peer to Peer Policy ..... 69
29. Personal Use Policy ..... 70
30. Physical Building Access Policy ..... 72
31. Remote Access Policy ..... 74
32. Risk Assessment Policy ..... 77
33. Router Security Policy ..... 78

**34. Server Security Policy ..... 80**
**35. System Hardening Policy ..... 83**
**36. Teleworking Policy ..... 85**
**37. Third Party Security Incident Reporting ..... 87**
**38. Vendor Management Audit Policy ..... 88**
**39. Vulnerability Detection and Security Patch Standards Policy ..... 89**
**40. Wireless Communication Policy ..... 90**
**41. Mobile Computing Policy ..... 91**

# Revision History

| Version | Author | Date | Changes |
|---|---|---|---|
| 1.00 | S. Nichols | July 1, 2011 | 1. Initial 1.0 Document |
| 1.01 | S. Nichols | July 31, 2011 | 1. Added Third Party Incident Reporting<br>2. Added Physical Security Policy<br>3. Added Data Recovery Policy |
| 1.02 | S. Nichols | September 6, 2011 | Editorial Revisions |
| 1.03 | S. Nichols | October 20, 2011 | Editorial Revisions |
| 1.05 | S. Nichols | June 20, 2012 | PII Additions |
| 1.06 | S. Nichols | July 10, 2012 | Teleworking policy added. |
| 1.07 | S. Nichols | January 16,2013 | Logo updated |
| 1.08 | R. Mayo | February 1, 2014 | 1. Changes to Remote Access Policy section 31.3.1<br>2. Changes to Physical Building Access Policy section 30<br>3. Change to Email and Communications Activities Policy section 3.4.5 |
| 1.09 | R. Mayo | June 2014 | Added Vendor Requirements Policy Section 38<br>• Vendor Risk Assessment<br>• Vendor Right to Audit |
| 1.10 | R. Mayo | September 2014 | • Added Mobile Computing Policy Section 41<br>• Added clarification on visitor escort policy Section 30.3.1 |
| 1.11 | R. Mayo | October 2014 | • Modified 29.3 Personal Use Policy |

# 1. INFOSEC Policy

## 1.1. Overview

DHI's INFOSEC group is committed to protecting DHI employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. The INFOSEC group is comprised of the Lead Security Administrator, his/her designates, and the CTO. This group carries out their security related duties as authorized by the CEO of DHI, Inc.

Effective security is a team effort involving the participation and support of every DHI employee and affiliate who deals with information and/or information systems. The INFOSEC Policies and Procedures in this document are the guidelines for behavior of every employee and contractor of the company with respect to security, both electronic and physical. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Additionally, it is the responsibility of every employee to report potential security violations or vulnerabilities when they are discovered. This may be done in person or via email. DHI routinely grants awards to employees selected by the Information Security Group as having played a significant role in improving the company's security.

## 1.2. Purpose

The purpose of this document is to provide employees and contractors of DHI with a clear understanding of the roles, responsibilities and authority of the INFOSEC group in granting exceptions to the INFOSEC policies, conducting security investigations and the potential enforcement that may result.

## 1.3. Scope

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

## 1.4. Exceptions

Exceptions to INFOSEC policies and procedures will rarely be granted and when granted will be for specific projects and limited time periods. It is recognized that situations may arise that require exceptions to certain INFOSEC policies. Requests for exceptions must be made in writing by the requestor and approved by the Lead Security Administrator and the CTO. Each exception granted may be subject to periodic review by the INFOSEC group in order to determine if the exception is still required.

## 1.5. Enforcement

Violations of INFOSEC policies may result in disciplinary action against the violator. INFOSEC will conduct investigations into potential violations. The results of such

investigations will be provided to the company's General Counsel. If further action is required, General Counsel may convene a disciplinary panel consisting of, without limitation, the manager of human resources and the CTO ("Disciplinary Panel").

If a Disciplinary Panel is convened, the Disciplinary Panel will review the results of the investigation to determine whether further action is required. If further action is required, the Disciplinary Panel will formulate a recommendation for disciplinary action. The results of the investigation and the recommendation shall be provided to the CEO of the company for final decision on disciplinary action. Disciplinary action shall be presented to the employee in the presence of the employee's direct supervisor and the manager of human resources.

## 1.6. Monitoring

Monitoring the company's security environment and conducting investigations into potential security problems are the responsibility and the duty of the INFOSEC group. Monitoring is an on-going daily activity that is conducted in-person and with automated tools that record events on a 7 X 24 basis.

In-person monitoring is conducted on a continuous basis by INFOSEC personnel, who are trained in observational skills (sometimes known as "situational awareness"), whenever they are present within the DHI offices. In-person monitoring is also conducted through manual review of event log files and video created by automated monitoring tools.

Automated monitoring is conducted on a continuous basis through the use of a variety of tools such as physical intrusion monitoring systems, video cameras with recording systems as well as network intrusion detection and decoy server systems (honeypots). Automated monitoring occurs on sources both external and internal to the company.

In the course of the on-going, daily monitoring, the INFOSEC personnel are primarily looking for events and behavior that are indicative of external attacks against the company's facilities and infrastructure. External attacks are dealt with by INFOSEC personnel in cooperation with outside assistance such as System Administrators at ISPs and the National Computer Emergency Response Team.

INFOSEC personnel are also charged with constantly looking internally for events and behavior that are inconsistent with INFOSEC policies. If an event or behavior of this type is detected, additional and more detailed investigation may result.

## 1.7. Investigations

Investigations begin with the detection of an incident (events or behavior by internal personnel) that is inconsistent with INFOSEC policies. Initially, INFOSEC personnel will determine if the incident is a general situation affecting the entire company (ex. Someone has invoked a virus that arrived attached to an email and it has spread throughout the company) or is the incident attributable to individual(s) (ex. An employee has attached an Excel spreadsheet with confidential information in clear text to an email and sent it outside the company).

If the incident is the broader situation affecting the entire company, INFOSEC may immediately initiate an investigation to devise and implement a solution as soon as possible. The CTO and General Counsel shall be informed of the investigation and kept apprised of progress on the solution. Policies and procedures may need to be

revised and company personnel may need to be trained to prevent further, similar incidents.

If the incident can be attributed to the actions of an individual or specific group of individuals, INFOSEC will document the incident and inform the CTO before beginning the investigation. The CTO shall consult with General Counsel and Human Resources to determine whether to proceed with a more detailed investigation.

If a decision to proceed is made, General Counsel shall provide INFOSEC guidance in conducting the detailed investigation. Human Resources will notify the appropriate managers that an investigation has been initiated. INFOSEC, acting at the direction of General Counsel, shall conduct the investigation using any and all tools legally available and approved by General Counsel. Investigations shall proceed as quickly as possible and all results shall be provided to the General Counsel. General Counsel, Human Resources and the CTO shall then initiate enforcement proceedings.

# 2. Acceptable Encryption Policy

## 2.1. Purpose

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

## 2.2. Scope

This policy applies to all DHI employees and affiliates.

## 2.3. Policy

Proven, standard algorithms such as 3DES, 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-Hillman, 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. DHI'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 U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

## 2.4. Definitions

- **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 is used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

# 3. Acceptable Use Policy

## 3.1. Overview

DHI's INFOSEC group is committed to protecting DHI's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. The INFOSEC group is headed by the Lead Security Administrator, who is responsible for the enforcement and policing of these policies. Any questions regarding authority, enforcement, or compliance with these policies should be addressed to the Lead Security Administrator.

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

Effective security is a team effort involving the participation and support of every DHI employee and affiliate who deals with information and/or information systems. It is the responsibility of every network user to know these guidelines, and to conduct their activities accordingly.

## 3.2. Purpose

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

## 3.3. Scope

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

## 3.4. Policy

### 3.4.1. General Use and Ownership

1. Users should be aware that the data they create on the corporate systems remains the property of DHI. Because of the need to protect DHI's network, management does not guarantee the confidentiality of information stored on any network device belonging to DHI.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use of company assets is governed by the Personal Use Policy.
3. INFOSEC recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see INFOSEC's Information Sensitivity Policy.

4. DHI may monitor equipment, systems and network traffic at any time, per INFOSEC's Audit Policy.
5. DHI reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 3.4.2. Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems (i.e. a web browser) should be classified as sensitive, confidential, or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in INFOSEC's Information Sensitivity Policy. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. 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.
4. Use encryption of information in compliance with INFOSEC's Acceptable Encryption policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Policy".
6. Postings by employees from a DHI email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DHI, unless posting is in the course of business duties.
7. Postings to newsgroups should never divulge specific information about the DHI network topology, applications, or business practices without prior approval from management.
8. All hosts used by the employee that are connected to the DHI Internet/Intranet/Extranet, whether owned by the employee or DHI, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
9. 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.

### 3.4.3. Unacceptable Use - Non-Exhaustive List

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an

employee of DHI authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DHI-owned resources.

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

### 3.4.4. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized release of any proprietary DHI data, applications, customer data, business plans, or any data whose release could reasonably be expected to cause financial harm to DHI.
2. Violations of the rights of any person or company or other entity protected by copyright, trade secret, patent or other intellectual property right(s), 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 DHI.
3. 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 DHI or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The General Counsel should be consulted prior to export of any material that is in question.
5. Introduction of maliCTOus programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. 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.
7. Using a DHI 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. The use of the DHI network to intentionally download pornographic images is expressly prohibited.
8. Making fraudulent offers of products, items, or services originating from any DHI account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. 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 maliCTOus purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to INFOSEC is made and approval received.
12. 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.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. 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.
16. Providing information about, or lists of, DHI employees or resources to parties outside DHI is strictly prohibited. This includes posting to technical support groups on the Internet. INFOSEC must authorize any exception to this rule in writing.
17. Installing unauthorized software onto machines within the DHI network. Authorized software is software that is distributed or approved by IT and INFOSEC. For example, a user downloading Weatherbug would not be installing authorized software, however a user installing Skype would. When in doubt contact IT or INFOSEC.

### 3.4.5. Email and Communications Activities

1. Effective February 1, 2014, access and use of personal email from the company network is strictly prohibited.
2. 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).
3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. 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.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within DHI’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DHI or connected via DHI’s network.
8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

# 4. Access Recertification Policy

## 4.1. Purpose

To establish INFOSEC policies regarding quarterly review of user access.

## 4.2. Scope

This policy applies to all employees and contractors operating within DHI.

## 4.3. Policy

Every three (3) months, INFOSEC will review the systems access of all users, and determine whether the users' current access levels are appropriate. In accordance with DHI's stated policies, all user access is granted on a "least access" basis. As such, any system access in excess of the minimal access required will be removed.

If a user feels he /she requires more system access than is deemed necessary by INFOSEC, the user must submit a written request, signed by a manager, stating why said access is required. Upon review of the request, INFOSEC and the Network Administrator will determine if a proper justification exists. Appropriate network access is always the final decision of INFOSEC.

# 5. Acquisition Assessment Policy

## 5.1. Purpose

To establish INFOSEC responsibilities regarding corporate acquisitions, and define the minimum-security requirements of an INFOSEC acquisition assessment.

## 5.2. Scope

This policy applies to any team charged with assessing all companies acquired by DHI and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

## 5.3. Policy

### 5.3.1. General

Acquisition assessments are conducted to ensure that a company being acquired by DHI does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. INFOSEC will provide personnel to serve as active members of the acquisition team throughout the acquisition process. The INFOSEC role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to DHI's networks. Below are the minimum requirements that the acquired company must meet before being connected to the DHI network.

### 5.3.2. Hosts

1. All hosts (servers, desktops, laptops) will be replaced or re-imaged with a DHI standard image.
2. Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by INFOSEC.
3. All PC based hosts will require DHI approved virus protection before the network connection.

### 5.3.3. Networks

1. All network devices will be replaced or re-imaged with a DHI standard image.
2. Wireless network access points will be configured to the DHI standard.

### 5.3.4. Internet

1. All Internet connections will be terminated.
2. When justified by business requirements, air-gapped Internet connections require INFOSEC review and approval.

### 5.3.5. Remote Access

1. All remote access connections will be terminated.
2. DHI will provide remote access to the production network.

### 5.3.6. Labs

1. Lab equipment must be physically separated and secured from non-lab areas.
2. The lab network must be separated from the corporate production network with a firewall between the two networks.
3. Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by INFOSEC.
4. All acquired labs must meet with DHI's network security policies, or be granted a waiver by INFOSEC.
5. In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the DHI Chief Information Officer (CTO) must acknowledge and approve of the risk to DHI's networks

## 5.4. Definitions

- **Business Critical Production Server** A server that is critical to the continued business operations of the acquired Company.

# 6. Anti-Virus and Malware Policy

## 6.1. Purpose

The purpose of this policy is to provide guidance to users to ensure the DHI network is adequately protected from computer viruses and worms and malware.

## 6.2. Scope

This policy applies to all DHI employees and affiliates.

## 6.3. Policy

DHI users should follow the following guidelines to prevent virus problems:

- Always run the standard, supported anti-virus software as distributed by the IT department. 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, in accordance with DHI's Acceptable Use Policy.
- Exercise extreme caution when downloading files from external sources. If there is any doubt about the source of the files to be downloaded, consult with INFOSEC.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette, CDROM or DVD 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. Backup of data on any of DHI's servers are the responsibility of the Network Support Group. Any files that a user wishes to be backed up on a regular basis should be placed in the "My Documents" folder on the user's workstation where they will automatically be backed up to the network.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, 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.
- New viruses are discovered almost every day. Daily updates of the virus definition database must be performed.

## 6.4. Definitions

- **Virus** A virus is a program that carries out a specific function and infects other programs in the process. In many cases the whole function of the virus is to replicate itself, nothing more. Other viruses rewrite data files making them useless.
- **Worm** A worm is a virus that does not infect other programs. It still replicates itself to other computers, but will always arrive in the same program.

# 7. Audit Policy

## 7.1. Purpose

To provide the authority for members of DHI's INFOSEC team to conduct a security audit on any system at DHI.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents to ensure conformance to DHI security policies
- Monitor user or system activity where appropriate.
- Further any other legitimate business interest of the company.

## 7.2. Scope

This policy covers all computer and communication devices owned or operated by DHI. This policy also covers any computer and communications device that are present on DHI premises, but which may not be owned or operated by DHI.

## 7.3. Policy

When requested, and for the purpose of performing an audit, any access required will be provided to members of DHI's INFOSEC team.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on DHI equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on DHI networks.

INFOSEC may also monitor network traffic and general use of internet and email,

# 8. Audit Logs Retention Policy

## 8.1. Purpose

The purpose of this policy is to establish and maintain an audit logs retention policy to enable proper forensic investigations of Infosec events.

## 8.2. Scope

This policy applies to all components within DHI.

## 8.3. Policy

In order to ensure the most secure computing environment as well as to comply with various regulations, DHI requires that all audit logs be kept for a minimum of two years wherever possible. Additionally, all deployed servers must be configured to send audit logs to the InfoSec log aggregator.

# 9. Automatically Forwarded Email Policy

## 9.1. Purpose

This policy states requirements to help prevent the unauthorized or inadvertent disclosure of sensitive company information.

## 9.2. Scope

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

## 9.3. Policy

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

## 9.4. Definitions

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

# 10. Bluetooth Communication Policy

## 10.1. Purpose

This policy prohibits use of unauthorized Bluetooth communications devices. Due to its insecure nature, ease of interception and data injection, and the type of devices that typically use Bluetooth, DHI prohibits use of said devices other than for voice communications unless specifically authorized by Infosec.

## 10.2. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) within DHI's facilities.

## 10.3. Policy

No Bluetooth devices, other than telephone headsets are to be used within any DHI facilities unless approved explicitly by Infosec, or unless Bluetooth connectivity has been disabled on the device.

Due to its inherent insecurity, anybody using Bluetooth headsets must ensure that no conversations that could contain sensitive information about our network such as configuration, usernames, security, or connectivity, be held over such a device. To be safe, all conversations about our network or client interactions should be held over a wired landline telephone.

## 10.4. Definitions

- **Bluetooth** A global initiative by Ericsson, IBM, Intel, Nokia and Toshiba to set a standard for cable-free connectivity between mobile phones, mobile PCs, handheld computers and other peripherals. It uses short-range radio links in the 2.gGHZ Instrumentation Scientific and Medical (ISM) "free band".

# 11. Change Management Policy

## 11.1. Purpose

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

## 11.2. Scope

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

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

- Periodic maintenance,
- Client requests,
- Hardware and/or software upgrades,
- Acquisition of new hardware and/or software,
- Changes or modifications to the infrastructure,
- Environmental changes,
- Operating system or vendor patches,
- Operations schedule changes,
- Changes in hours of availability, and
- Unforeseen events.

The above list is not all-inclusive. Therefore, if you are unsure if a change needs to be submitted through the Change Management process, you should contact the DHI Change Management Administrator.

## 11.3. Policy

DHI managers are responsible for pro-active planning in managing their environments. Change Requests should be submitted as soon as all planning has been completed, but no later than the mandatory deadline of two (2) business days prior to a CCB meeting.

Managers are encouraged to develop internal policies, procedures, and additional checklists to enhance and support the overall Change Management Policy and Procedure. An example of a checklist can be found in Appendix A and is provided for

managers to use as a guideline to ensure the Change Management Policy and Procedures are adopted and the appropriate research is completed, prior to submitting a Change Request to the Change Control Board (CCB). Please note this list is not intended to be all-inclusive.

### 11.3.1. Submission of a Change Request

1. The Requester must obtain management approval prior to submitting a request. This ensures that managers are aware of all changes occurring in their areas of responsibility.
2. All Change Requests shall be submitted on the Change Request Form located online in the public forms folder.
3. The Change Request must include enough detail so that all areas know the relative impact of the change and how it may affect other areas. Change Request Forms not completed properly will be rejected and returned to the Requester with an explanation for the denial.
4. The Change Request Form shall be submitted no later than two (2) business days prior to the CCB meeting where it will be considered.
5. Each request will be discussed at the regularly scheduled Change Control Board meeting (to be held at least once a month, but not more often than once a week). After approval at CCB, changes can, but not necessarily must commence the following day.
6. The CCB will send out a notification of the next meeting date immediately following each meeting via email.
7. Change Requests can be submitted up to 3 months prior to the change to be made.
8. A request can be submitted for non-critical recurring processes that need to be implemented on an ongoing basis (ex. Regular changes of admin passwords on systems). Such request shall be submitted, discussed and approved once, although they may be discussed prior to each execution of the work. Once approved, the required process shall be set up as a recurring task to alert the appropriate personnel when it needs to be executed.

If a change is submitted and is in conflict with a previously scheduled change, the change will not be posted and the Change Control Board will notify the parties of the conflict. The first requested change will remain posted until the parties notify the Change Control Board of the resolution in writing, preferably by email, before the CCB meeting.

If the parties cannot reach an agreement, the issue shall be elevated to the Vice President of Operations for resolution, and again the resolution is to be submitted to the CCB prior to the meeting.

**NOTE:** Operations reserves a window each Sunday morning from 2:00 a.m. to 5:00 a.m. Pacific Time for WAN, LAN and server maintenance. This window will be strictly guarded for this purpose. However, all changes performed during the maintenance window shall be scheduled through the Change Management Process. Any changes requested for this time period for any other reason must include a business case for doing so, and will be approved/denied on a case by case basis. The CCB will see that these exceptions are discussed with the managers from the Network Support and Security Administration staff, and coordinated accordingly.

See Appendix B for Urgency of Change definitions.

See Appendix C for examples of Types of Changes.

### 11.3.2. Updating, Correcting, or Withdrawing a Change Request

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

## 11.4. Emergencies

Emergencies exist only as a result of:

- Consumers are completely out of service,
- there is a severe degradation of service needing immediate action,
- a security vulnerability/condition that can be mitigated by installing a critical vendor supplied security patch,
- a system/application/component is inoperable and the failure causes a negative impact,
- a response to a natural disaster, or
- a response to an emergency business need.

All emergencies, which shall include program moves, (routine program moves do not qualify as an emergency), are handled on an as-required basis with the approval of the Vice President of Operations, or designee, and must follow the guidelines below:

1. Send an emergency approved Change Request Form to the CCB either before or immediately after the change occurs.
2. The Vice President of Operations (or his/her designee) will notify the CCB the Network Support staff of the emergency change. The notification shall include at a minimum the following information:
    - Will the change cause an interruption in service?
    - What additional clients will be affected (in the event a change is needed to fix an outage) and who needs to be notified by the Network Support staff?
    - What is the possible work around until the problem is resolved?
    - What is the approximate length of the outage?
    - Notification of resolution.
    - Completion of a Bugzilla entry to accurately describe the outage.

Emergencies after normal business hours, on the weekend or holidays, will be resolved immediately and reported to Network Support Manager as he is responsible for after-hour coverage. A bug tracking systems entry will be generated and staff will notify affected clients, as applicable. A completed Change Request Form must be submitted through the regular reporting process on the first work day immediately following when the change was made.

The CCB will review all emergency submissions to ensure the change met the criteria for an "emergency change" and to prevent the process from becoming normal practice to circumvent the Change Management Process. Any questions will be directed to the manager who approved the change.

## 11.5. Vendor Change Requests

Vendors that control portions of the infrastructure will be encouraged to submit change notifications to the designated DHI contact. The DHI contact is responsible for evaluating and submitting those changes to CCB on the Change Request Form, following the same procedures as an internal submission. They will be encouraged to send the notifications to the Manager of Network Support, who will evaluate the request, complete the DHI Change Request Form, and submit the request through the normal process.

## 11.6. Change Control Board Meeting

A CCB meeting will be held as required (all interested parties to be notified by e-mail) and will be facilitated by the Chairperson Change Control Board (CCB) or designee.

### 11.6.1. Purpose

The purpose of the meeting is to share information, concerns, comments, etc. in a cooperative environment in order to eliminate potential disruptions of service to DHI clients. The primary objectives to be accomplished at each meeting are as follows:

- Review last changes implemented and discuss any pertinent issues or problems encountered. The CCB will document and follow the change through to completion.
- Review proposed changes received since the last meeting.
- Identify conflicts and ask for resolution from parties involved.
- Establish if consumers and partners are affected by the requested change and if procedures are in place for notifying them once change is approved.
- Review and request resolution from requestors, if the change overlaps and/or conflicts with another requested change.
- Schedule a time frame to implement a change, while considering application restrictions and upcoming events such as month end, year-end, holiday, heavy volume days, that is, any justified business need.
- Ensure availability of a back-out or fallback plan.

- Ensure support is defined and appropriate staff are available in the event of a back-out to the change or a related problem.
- Finalize and approve up-coming changes.
- Review and discuss future changes that have been requested and the impact of those changes.

### 11.6.2. Participants

All departments that have the potential to make changes to any component that could have an impact on the production infrastructure are required to send a representative to the CCB meeting. In addition, any individual that has submitted a Change Request for that meeting must attend, or send a designee who has knowledge of the change.

The Chairperson of the CCB shall be the Vice President of Operations (or designee). The minimum attendees at any CCB meeting must include a representative from Product Management, Network Support, Implementation, Security and Software Development.

The staff present at the meeting makes up the CCB for that meeting and will be encouraged to ask questions concerning the changes.

If there is not a representative at the meeting for a requested change, the change will not be scheduled. A new Change Request Form will have to be submitted.

## 11.7. Responsibilities

### 11.7.1. Chairperson of Change Control Board

The CCCB will direct the Change Management Process, which will include facilitating the scheduled CCB meetings and publishing the schedule of subsequent meetings.

The CCCB responsibilities include the following tasks:

- Schedule and conduct CCB meetings.
- Analyze and evaluate a Change Request as it relates to the impact on DHI production infrastructure.
- Approve or deny the change schedule in accordance with the DHI Change Management Policy and Procedures, and report any deviations to the appropriate manager and/or to the requestor.
- Perform impact/risk analysis to eliminate potential conflicts.
- Coordinate the changes/events.
- Notify parties of conflicts needing resolution.
- Post the change schedule.
- Send out notifications of any emergency changes in the event the new schedule has already been posted.

The updated Change Management Schedule will be posted after each CCB. Among other items, the web posting will list the current changes, each with a contact person and an implementation date.

### 11.7.2. Change Requestor

It is the primary responsibility of the individual submitting a request to evaluate the change prior to submission. The requestor should also review previously scheduled outages/events that may affect his/her requested change.

The Change Requestor's responsibilities include the following tasks:

- Perform risk benefits/risk analysis.
- Verify that all equipment, software, hardware, and updates are available.
- Research the requirements to achieve a successful change (required patches and stability of upgrade).
- Evaluate the impact to the system/network and to the clients.
- Document and coordinate a fallback plan. This should explain the steps that must be taken to restore access in the event that the change has a negative impact. (This is to be presented at the CCB meeting).
- Develop a plan of action to reduce the risk to an acceptable level. (This plan requires a manager's approval and will also be reviewed at the CCB meeting).
- Develop a plan of action to lessen the affects on the client if the change should cause an outage.
- Complete any internal checklist that may be required by the manager.
- Obtain approval from the manager or designee for requesting the change.
- Submit a complete, concise, and descriptive Change Request Form no later than two business days prior to the CCB meeting where the change will be considered. Change Request Forms not completed properly will be rejected and returned to the requestor with an explanation for denial.

Once the request is approved:

- Ensure that the client is aware of any possible impact.
- Coordinate proper on-site or on-call support as needed to resolve any problems or answer any questions that may occur during installation, or immediately subsequent to installation. Contact names and numbers should be available to Network Support staff to obtain additional or outside support.
- Report unplanned outages or problems immediately through the Manager of Network Support.
- Provide a status update in the "Change Results" section of the Change Request Form with the manager's or designee's approval, upon completion of the requested change. The completed form must provide an update on the success or failure of the change in detail.

NOTE: Changes to systems should never be implemented on Fridays (or the last day of business on a holiday weekend), to ensure proper troubleshooting resources are on-hand to address any resulting problems.

## 11.8. Unplanned Outages

All unplanned outages shall be reported to the Manager of Network Support immediately and will be captured through the bug tracking systems system. For any

major outages, an Outage Review report will be available within 36 hours of the resolved outage. The Outage Review will include such information as the type of outage, down time, clients affected, and resolution. Managers are encouraged to provide accurate details of the problem and resolution in the bug tracking system entry to facilitate the reporting process. Cooperation and participation is required from all levels of management and staff to facilitate generating this report.

## 11.9. Definitions

- **Change** To transform, alter, or modify the operating environment or standard operating procedures; any modification that could have a potential and/or significant impact on the stability and reliability of the infrastructure and impacts conducting normal business operation by our clients (both internal and external); any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.
- **Event** Any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period.
- **Change Request** The official notification of the change/event submitted via the Change Request Form.

## 11.10. Appendices

## 11.10.1. Appendix A: A Guideline for an Internal Checklist

- Risk benefits/risk analysis has been completed.
- All equipment, software, hardware, and updates are available.
- Requirements to achieve a successful change (required patches and stability of upgrade) have been researched.
- The impact to the system/network and to the clients has been evaluated.
- Fallback plan is documented. This plan explains the steps that must be taken to restore access in the event that the change has a negative impact. Required for CCB meeting wherever possible.
- Plan of action to reduce the risk to an acceptable level has been completed. This plan requires a manager's approval and will be reviewed at the CCB Meeting.
- Plan of action to lessen the affects on the client if the change should cause an outage is completed.
- Change Request Form is complete, concise, includes a detail description, and is submitted on time.
- If approved, client has been notified of any possible impact.
- On-site or on-call support as needed to resolve any problems or answer any questions that may occur during installation, or immediately subsequent to installation has been coordinated. Contact names and numbers have been made available to support staff to obtain additional or outside support.

- Any unplanned outages have been reported to the Manager of Network Support.
- A status update in the "Change Results" section of the Change Request has been completed and submitted.

## 11.10.2. Appendix B: Urgency of Change:

- **Emergency** The problem requires immediate attention where either system failure or mission essential requirements are not available and no work around exists. This problem can apply to the system as a whole or to a particular site if system access is lost. This type of Change Request will receive an immediate initial analysis; however, the initial analysis is not mandatory for approval. The corrective action is implemented as soon as the fix is available regardless of change management schedule, however appropriate organizational reviews and approvals must be submitted to change management as soon as possible. Resolving and implementing a fix to a Priority 1 problem is worked until completed.
- **High/Urgent**The problem is of an urgent nature and can justify an out-of-cycle change. This priority is used for problems that meet the Priority 1 requirements, except that a work around exists, or performance degradation for which no temporary work-around is available however delay would not cause adverse mission impact beyond that of inconvenience. These changes must still be controlled, tested and approved prior to implementation on a production system. Change Requests that fall into this category may, at the approval of the manager be submitted after the CCB deadline for final analysis, coordination and schedule inclusion.
- **Medium** Routine Change Requests are judged less operationally important than Priority 2 or the time frame is not critical for implementation. This priority may be used for important software/hardware/network maintenance issues such as version upgrades, utility software, etc. This priority may be used to improve very difficult or awkward implementations for heavily used subsystems on a selective basis. This priority may be used for development activity or new requirements providing that the activity cannot be accomplished with the lower priority. These problems are resolved and implemented in the next scheduled change cycle.
- **Low** This priority is intended primarily for new requirements and for fixing capabilities that are currently operational but are difficult or awkward to use. It applies also to non-standard implementations, and other assorted irritants.

The manager, prior to submission to the CCB, will determine the priority of the change. The CCB has final determination as to the correct priority of each Change Request.

## 11.10.3. Appendix C: Types of Changes:

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

1. **Computing Systems Hardware** Hardware changes, additions, deletions, re-configurations, re-locations, preventive, or emergency maintenance.

2. **Computing Systems Software** Program Temporary Fixes (PTFs), product releases, versions, I/O and Network Control Program (NCP) gens, table changes, tuning, alterations to libraries, catalogs, monitors, traps, or changes to priority mechanisms, job classes, print classes.
3. **Environmental** Power, UPS systems, generators, air conditioning, electrical work, facility maintenance, security systems, fire control systems.
4. **Network Systems** Additions, modifications, deletions to lines, modems, routers, network access, controllers, servers, protocol converters. Software components either distributed or centralized, translators, router software, printing routines, servers.
5. **Applications and Information Systems** Implementation of new applications, disk volume changes, new systems, new releases, or modifications. Migration from test to production of source code.
6. **Operating procedures** Changes in equipment downtime schedules, planned system outages, changes in delivering services, or changes to service levels.
7. **Shared Servers and Public Folders** Changes in hours of availability, hardware configurations, operating systems, utilities, applications including release levels or versions, installations or de-installations of systems, servers.

# 12. Contractor Access Policy

## 12.1. Purpose

To establish INFOSEC policies regarding access to facilities, documents and resources for external contractors operating within the DHI environment.

## 12.2. Scope

This policy applies to all non-employees operating within DHI. From time to time, there will be requirements for personnel other than DHI, Inc. employees to be present and conduct work within the offices and datacenters of DHI. Due to the sensitive nature of the data that is stored and processed within the confines of DHI offices or datacenters, the following document sets forth the rules that shall be followed when anyone other than an employee requires access to the offices or datacenters to conduct work. This policy is meant to specifically differentiate between a "visitor" and someone who is conducting work on behalf of DHI or at the request of DHI.

The following list of situations potentially requiring access for non-employees is provided as examples and is not meant to be exhaustive:

a. • External firms conducting financial or security audits.

b. • Consultants/contractors performing contractual services of any kind.

c. • Personnel from external firms demonstrating software/hardware for evaluation by DHI personnel.

d. • Personnel from external firms conducting training of DHI personnel.

e. • Personnel from clients attending training sessions conducted by DHI.

f. • Personnel from external firms performing repair services of any kind.

g. • Personnel from external firms performing cleaning, plant maintenance or preventive maintenance on company owned equipment of any kind.

h. • Personnel from external firms performing catering services of any kind.

There are potentially many other reasons for non-employees to require access to the offices and datacenters of DHI that cannot be listed in advance. The general rule that every DHI employee should follow is to assume that any time a non-employee requires access for any reason, it is a situation covered by this policy.

The following rules are divided into two categories: rules governing authorization for a non-employee to be granted access for work and rules governing non-employees and their behavior once authorized for work.

## 12.3. Policy

### 12.3.1. Before Non-employee Begins Work

Note: All Non-employees are required to sign the company's standard Non-Disclosure Agreement prior to commencement of work.

### 12.3.2. Work engagements must be initiated with a legal document.

- Before a non-employee is granted access to the DHI offices or datacenters, a Non-Employee Access Request document shall be completed. This document is available through Outlook Public Folders under "Forms", or upon request from the Lead Security Administrator. The document must be completed fully, including a description of the scope of work to be performed, system and physical access required, the length of time access is required, and the number of non-employees that will require access for the proposed task.
- The document shall be signed by the requesting supervisor, an executive sponsor (VP level or above), the Lead Security Administrator, and the President/CEO.
- The document will be submitted to the Lead Security Administrator at least five full business days before work is to commence in order to ensure that the appropriate access is granted in a timely fashion.
- The executive sponsor or designated employee shall submit to the Lead Security Administrator an e-mail request for all required system accounts, e-mail accounts and electronic access cards/fobs at least 2 full business days prior to arrival of non-employees to begin work.
- If the work engagement will require DHI to furnish computer equipment, telecommunication equipment or dedicated work space (vs. temporary seating) an e-mail request shall be submitted to the Network Support Manager at least 5 business days prior to arrival.

### 12.3.3. Work engagements must be sponsored by a senior executive of DHI.

- While any supervisory-level personnel may request access for contract or consulting personnel, such personnel must be sponsored by a Vice President-level employee or higher.
- The executive sponsor may delegate responsibility to other employees for
- explaining rules of behavior while working in the offices and responsibility for monitoring of non-employees behavior while working, but the sponsor shall be held ultimately responsible for the actions of the sponsored non-employees and the employee to whom monitoring tasks have been delegated.
- Identity badges

- When implemented, identity badges shall be furnished to each non-employee with authorized access to DHI office spaces. The Lead Security Administrator shall be solely responsible for issuing orange contractor badges without picture or orange contractor badges with picture at his discretion.
- Non-employees will not be granted access to DHI datacenters unless they possess an appropriate identity badge as previously mentioned.

### 12.3.4. Sign-in and sign-out at front desk

- Non-employees shall sign in and sign out at the front desk in the DHI lobby at the beginning and end of every working day.
- Non-employees shall prominently display the furnished identity badge at all times while working in the DHI office spaces.

### 12.3.5. Working hours

- Non-employees shall be restricted to working hours of 8:00am through 5:00pm Monday through Friday excluding holidays unless specifically authorized to work extended hours by the Lead Security Administrator.
- Non-employees may not work in the DHI offices spaces after normal working hours, on official company holidays or on weekends unless accompanied AT ALL TIMES by the executive sponsor or the designated representative.

### 12.3.6. Access beyond the DHI lobby

- An electronic access card/fob may be requested for a non-employee on the Non-Employee Access Request form. This request may be granted at the sole discretion of the Lead Security Administrator. If such device is issued to non-employee, that Lead Security Administrator is responsible for informing lobby receptionist that non-employee has been granted access.
- If the non-employee is not granted access to the facilities as described above, once a non-employee signs in at the front desk, the receptionist shall call the executive sponsor or designated representative who will escort the non-employee into the office spaces beyond the lobby.
- If a non-employee without access leaves the DHI offices for any reason during the regular working day, it is the responsibility of the executive sponsor or designated representative to escort them back into the office spaces beyond the lobby should they return, unless an electronic access card/fob has been issued.
- DHI reserves the right to search Non-employee bags, brief cases and or any other containers any time the non-employee leaves the premises.

### 12.3.7. Access to data center, secure tape storage and secure mail room

- Non-employees shall not have unsupervised access to the DHI data center nor the secure Tape Storage Room/Secure Mail Room at any time.

- Under certain circumstances, personnel from external companies may require access to the data center to perform maintenance or repairs. The Vice President of Operations and the Lead Security Administrator shall be responsible for determination of when external contractors are to be granted access to the data center.
- Non-employees working in the data center shall be escorted AT ALL TIMES by an DHI employee.
- Under certain circumstances, personnel from external companies may require access to the secure tape storage room/secure mail room to perform maintenance or repairs. The Vice President of Operations and the Lead Security Administrator shall be responsible for determination of when external contractors are to be granted access to the secure tape storage room/secure mail room.
- Non-employees working in the secure tape storage room/secure mail room shall be escorted AT ALL TIMES by an DHI employee.

### 12.3.8. Access to DHI internal network

- Access to the internal network for non-employee working within the DHI office spaces shall be solely at the discretion of the Lead Security Administrator and shall be restricted to a specially configured VLAN for non-employees only.
- Non-employees shall not have access to the back-office VLAN, the development VLAN or the production VLAN under any circumstances. Should a non-employee working within the office space require access to any data resident on the restricted VLANs, arrangements must be made with the Manager of Network Support to move the data to private folders that can be accessed from the special non-employee VLAN.
- Non-employees shall not have external access to the internet unless specifically authorized by the Lead Security Administrator.
- Non-employees shall not have remote access, through VPN or RAS or other similar methods, to DHI internal networks or computer resources under any circumstances without express written permission from the President/CEO.
- Non-employees shall be restricted to using specially configured workstations that have no peripherals capable of recording data (no write-able CDROM or DVD, no floppy drive, no active USB ports). These workstations shall be configured with password protection on the ROMBIOS.
- Computer equipment not owned and configured by DHI may not be attached to internal networks under any circumstances without express written permission from the President/CEO.
- Non-employees shall not have access to printers unless specifically authorized by the Lead Security Administrator.

### 12.3.9. Access to confidential data

- Confidential data is defined as data provided to DHI by our clients. Confidential data is defined as data relating to DHI's day-to-day business which would be of value to our competitors.

- Non-employees shall not have access to sensitive data under any circumstances without express written permission from the President/CEO.
- Non-employees may be granted access to confidential data at the request of the executive sponsor and at the discretion of the Lead Security Administrator and only if they have signed the company's standard Non-Disclosure Agreement.
- Non-employees are forbidden from removing any form of data, on any media, including but not limited to print, CD, DVD, USB key, memory card, etc., from the DHI office spaces.
- If non-employees are granted access to a printer, the executive sponsor or designated representative is responsible for ensuring that printouts of any confidential data output by the non-employee are properly accounted for, properly protected from disclosure and properly discarded for shredding when no longer needed.
- Non-employees and any containers they bring to the DHI office spaces are subject to search any time they are exit the offices spaces and DHI reserves the right to conduct such searches.

## 12.3.10. Once non-employee Completes Engagement

- Executive sponsor or designated representative is responsible for ensuring that all confidential material accessed by non-employee is properly accounted for, properly returned to appropriate protected status or properly discarded for shredding, if appropriate.
- Executive sponsor or designated representative is responsible for informing Lead Security Administrator and Network Support Manager that work engagement has ended. This notification shall be via e-mail.
- Executive sponsor or designated representative is responsible for collecting any electronic access card/fob that may have been provided to non-employee and returning that device to Lead Security Administrator.
- The Manager of Network Support shall be responsible for recovery of any company owned computer resources used by non-employee during work engagement and disabling any network access that may have been granted to non-employee.
- The Lead Security Administrator shall be responsible for informing lobby receptionist that non-employee is no longer authorized access to DHI office spaces.

# 13. Data Security Policy

## 13.1. Purpose

The purpose of this policy is to establish standards for the use of potentially sensitive data within the DHI network, particularly for use of data warehousing and data analysis. Effective implementation of this policy will minimize the risk of unencrypted data remaining at rest on our network.

## 13.2. Scope

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

## 13.3. Policy

### 13.3.1. Movement of sensitive data

When data is required for testing, warehousing, or analysis, a written request must be made to the data manager for approval. Data manager will then

- open a data request ticket
- coordinate the movement of data from whatever host said data resides on to data manager's staging system
- decrypt said data with data's keys
- encrypt data with requesting group's keys, while ensuring sensitive data remains encrypted in the resulting file
- data will then be staged onto requesting group's host
- upon requesting group's completion of data study, the data is to be erased and the data manager notified
- data manager will not close request ticket until he/she has verified data has been erased

### 13.3.2. Compliance

Audits will be performed on a regular basis by authorized organizations within DHI such as InfoSec.

### 13.3.3. Definitions

- **Sensitive Data** Any data that needs to be encrypted as per federal, state, or contractual guidelines/regulations

# 14. Data Recovery Policy

## 14.1. Purpose

All electronic information which is critical to support the production environment must be copied onto secure storage media on a regular basis (i.e., backed up), for the purpose of disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

## 14.2. Scope

Data custodians are responsible for providing adequate backups to ensure the recovery of electronic information in the event of failure. These backup provisions will allow DHI Production environment to be resumed in a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple generations of backups should be maintained.

Federal and state regulations pertaining to the long-term retention of information (e.g., financial records) will be met using separate archive policy and procedures, as determined by the Business Owner of the information, and in accord with the Records Management Program. Long-term archive requirements are beyond the scope of this policy.

## 14.3. Policy

- Backups of all DHI data and software must be retained such that computer operating systems and applications are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
- At a minimum, one fully recoverable version of all DHI Records must be stored in a secure, off-site location. An off-site location may be in a secure space in a separate building, or with an off-site storage vendor approved by the CTO.
- Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
- All DHI Data accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. DHI Data located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives. Alternatively, DHI Data located directly on workstations, laptops, or other portable devices may be backed up using a 3rd party vendor approved by the Information Technology Security Office.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to

perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.

- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested on an annual basis.

# 15. Employee Education Policy

## 15.1. Purpose

The purpose of the Employee Education Policy is to provide new hires with an initial understanding of all DHI's InfoSec Policies and to provide current employees with annual training to reinforce DHI's InfoSec Policies.

## 15.2. Scope

This policy applies to all current employees and all new hires.

## 15.3. Policy

The Lead Security Administrator will conduct the onboarding training for new employees and will be responsible for scheduling and training all current employees on an semi-annual basis.

# 16. Encryption Standards Policy

## 16.1. Purpose

The purpose of this policy is to establish and maintain an encryption configuration within the DHI environment.

## 16.2. Scope

This policy applies to all components within DHI.

## 16.3. Policy

In order to ensure the most secure computing environment as well as to comply to various regulations, DHI requires that all transactions involving sensitive data be encrypted. As such we support the following encryption standards:

3DES, SSL, PPTP, IPSEC, AES, Blowfish, Psypher, PGP, GPG

We will support any vendor who implements any of the above protocols.

## 16.4. Enforcement

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

# 17. Extranet Policy

## 17.1. Purpose

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

## 17.2. Scope

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

## 17.3. Policy

### 17.3.1. Pre-Requisites

### 17.3.2. Security Review

All new extranet connectivity will go through a security review with the Information Security department (INFOSEC). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

### 17.3.3. Third Party Connection Agreement

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

### 17.3.4. Business Case

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

### 17.3.5. Point Of Contact

There must be a person within DHI designated to be the Point of Contact (POC) for the Extranet connection. The POC is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

### 17.3.6. Establishing Connectivity

Groups within DHI that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage INFOSEC to address security issues inherent in the project. If the proposed connection is to terminate within the internal network at DHI, the INFOSEC group must be consulted. INFOSEC must be provided full and complete information as to the nature of the proposed access to the extranet group as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. DHI shall have sole responsibility for protecting DHI's network or resources and shall not rely on any Third Party for same.

### 17.3.7. Modifying or Changing Connectivity and Access

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

### 17.3.8. Terminating Access

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

### 17.3.9. Definitions

- **Circuit** For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.
- **Sponsoring Organization** The DHI organization who requested that the third party have access into DHI.
- **Third Party** A business that is not a formal or subsidiary part of DHI.
- **Third Party Agreement** An Agreement between DHI and Third Party outlining terms and conditions for extranet connectivity.

# 18. Firewall Policy

## 18.1. Purpose

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset.

Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities.

Firewalls are typically categorized as either "Network" or "Host": a Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly.

This policy statement is designed to:

- Provide guidance on when firewalls are required or recommended. A Network Firewall is required in all instances where Sensitive Data is stored or processed; a Host Firewall is required in all instances where Sensitive Data is stored or processed and the operating environment supports the implementation. Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.
- Raise awareness on the importance of a properly configured (installed and maintained) firewall.

## 18.2. Scope

## 18.3. Policy

Where Electronic Equipment is used to capture, process or store data and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is required.

All installations and implementations of and modifications to a Network Firewall and its Configuration and Ruleset are the responsibility DHI Firewall Administrator.

Where Electronic Equipment is used to capture, process or store data identified as DHI "Legally/Contractually Restricted" and the Electronic Equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is required where the operating environment supports that installation. The maintenance of the Host Firewall's Configuration and Ruleset is the responsibility of that system's administrator.

Where Electronic Equipment is used to capture, process or store data identified as DHI Public and the Electronic Equipment is accessible via an Internet connection, a Host and/or Network Firewall is recommended.

Use of a Host Firewall is recommended for any individual Host with access to the Internet; its maintenance is the responsibility of the individual user or designated support personnel.

All Network Firewalls installed and implemented must conform to the current standards as determined by DHI. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

1. Request and document all changes to Network Firewall Rulesets where Firewall Administration is performed by DHI. All requests are subject to the approval of DHI and review by ISS/C or its designate.
2. All related documentation is to be retained by the Firewall Administrator for three (3) years and is subject to review by DHI and Audit and Advisory Services.
3. All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default (the initial Ruleset should be set to “logging or learning mode” to prevent service interruptions). The Ruleset should be opened incrementally to only allow permissible traffic.
4. Firewalls must be installed within production environments where “Legally/Contractually Restricted Information” is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.
5. Firewall Rulesets must be configured to deny all traffic from “untrusted” networks\hosts (except http port 80, SSL port 443), SSH or VPN) unless a specific justification is made in writing for specific port access.
6. Firewall Rulesets and Configurations require periodic review to ensure they afford the required levels of protection:
    - DHI must review all Network Firewall Rulesets and Configurations during the initial implementation process.
    - Firewalls protecting Enterprise Systems must be reviewed semi-annually.
    - Firewalls not protecting Enterprise Systems must be reviewed annually by the responsible Firewall Administrator.
    - Firewall Administrators must retain the results of Firewall reviews and supporting documentation for a period of three (3) years; all results and documentation are subject to review by DHI and Audit and Advisory Services.

- Firewall is required to implement NAT for IP address translation to prevent any internal IP address from leaving the internal DHI network
- Firewall Rulesets will be configured to deny all traffic from “untrusted” networks/hosts where passwords could be transmitted in clear text (e.g. FTP, telnet)

- Firewall Rulesets must utilize groups and roles is the assignment of the firewall ruleset
- Firewall Rulesets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.
- Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternate storage (not on the same device) and reviewed at least daily, with logs retained for ninety (90) days. It is recommended that utilities or programs that facilitate the review process be employed. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.
- DHI Firewall Administrators will execute approved changes to the Firewall Rulesets maintained by DHI during the scheduled maintenance window.
- DHI Firewall Administrators will perform changes to Firewall Configurations according to approved production maintenance schedules.

## 18.4. Definitions

- **Electronic Equipment** All DHI-owned or issued and any personally-owned computer or related equipment (e.g., servers, workstations, laptops, PDAs, printers, fax and other such devices) that attaches to the DHI network, or is used to capture, process or store DHI data, or is used in the conduct of DHI business.
- **Enterprise System** Applicable to any infrastructure as a means of describing its importance to the DHI Production Environment and how it should be administered, protected and funded. From a functional viewpoint, an Enterprise System will be either (a) the only delivery platform for an essential service, or (b) a platform for a service to a very broad constituency spanning organizational boundaries. An Enterprise System is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered.
- **Firewall** Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.
- **Firewall Administrator** The DHI function charged with the responsibility of Firewall Configuration and/or Ruleset administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rulesets.
- **Firewall Configuration** The system settings affecting the operation of a firewall appliance.
- **Firewall Ruleset** A set of policy statements or instructions used by a firewall to filter network traffic.
- **Host**: Any computer connected to a network.

- **Host Firewall**: A firewall application that addresses a separate and distinct host. Examples include, but are not limited to: Symantec's Norton Personal Firewall, Zone Labs' ZoneAlarm, native firewall functionality supplied under operating systems, e.g., Mac OS X, Linux, Windows XP, Windows Vista.
- **Internal Information** Information that is intended for use by and made available to employees of DHI who have a business need to know. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business need. DHI reserves the right to control the content and format of Internal information when it is published to external parties
- **Legally/Contractually Restricted Information**: Information that is required to be protected by applicable law or statute (e.g., FCRA,DPPA), third party contract, or which, if disclosed to the public could expose the DHI to legal or financial obligations. Examples include, but are not limited to, occurrences of personally-identifiable information, e.g., social security numbers (SSNs), driver's license number and credit card numbers.
- **Network Device** Any physical equipment attached to the DHI network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points.
- **Network Extension** Any physical equipment attached to the DHI network designed to increase the port capacity (number of available ports) at the point of attachment. Examples include, but are not limited to: routers (wired and wireless), switches, hubs, gateways.
- **Network Firewall** A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).
- **Public Information** Information that is available to all employees of DHI, and may be released to the general public. DHI reserves the right to control the content and format of Public Information. This information is not restricted by local, state, national, or international statute regarding disclosure or use.
- **Sensitive Data** See "Legally/Contractually Restricted Information" above.
- **DHI Network** The network infrastructure and associated devices provided or served by DHI.

# 19. General Host Configuration Standards Policy

## 19.1. Purpose

The purpose of this policy is to establish and maintain a configuration standard for non-server machines deployed within the DHI network.

## 19.2. Scope

This policy applies to all network components identified as critical infrastructure.

## 19.3. Policy

In order to ensure the most secure computing environment, it is essential that all critical systems adhere to a configuration standard. This standard states that all said systems shall:

- all installations must adhere to the corporate security policies and procedures
- run only required services;
- log user access;
- have the most current patches and firmware;
- only allow listening services that are critical for basic functionality;
- implement only secured listening services (ie. ftp and telnet not allowed);
- all vendor supplied defaults must be changed prior to installation on the DHI network (e.g. passwords, elimination of unnecessary services, etc.)
- minimal user access provisions;
- strong passwords with lockout following 5 incorrect passwords;
- all systems shall log to a centralized log aggregator
- systems shall be configured to automatically download patches; installation of patches should be set for manual intervention
- additional packages can be installed as required by INFOSEC or IT – all such packages shall be logged in the change control logs.
- Each system should be configured to perform only one primary function where practical.

# 20. Incident Reporting Policy

## 20.1. Purpose

The purpose of this policy is to provide guidance for DHI employees and their responsibility to report potential violations of our corporate InfoSec polices and procedures, state/federal regulations or laws, or potential breaching of contractual obligations.

## 20.2. Scope

This policy applies to all DHI employees and affiliates.

## 20.3. Policy

In order to ensure our compliance with various federal and state regulations, as well as to ensure our clients are abiding by our contractual agreements, all employees are required to report to InfoSec or the CTO any occurrence of unencrypted confidential data being sent via email or other computer connection to our network. "Confidential data" refers to consumer data that contains a consumer name in conjunction with any government issued number, account number, credit card number, or date of birth. Additionally, any occurrence of a client sending data in a manner not agreed upon must also be reported to either InfoSec or the CTO. Any such incident must be reported to InfoSec within one business day of the incident occurring.

All employees are also required to report any discovered potential vulnerabilities regarding operating system or application configuration, or any lapse in physical security. Any such vulnerabilities must be reported to InfoSec within one business day of discovery.

# 21. Information Sensitivity Policy

## 21.1. Purpose

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

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

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

Note: All Confidential Information (defined below) shared with any person or entity outside of DHI shall not be shared unless and until a fully executed copy of the appropriate Non-Disclosure Agreement is received by DHI Legal. It is the responsibility of each DHI employee seeking to share such Confidential Information to ensure no Confidential Information is shared absent a Non-Disclosure Agreement. Questions regarding the use of Non- Disclosure Agreements and/or how to obtain the DHI's approved form Non- Disclosure Agreements should be addressed with Legal.

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.

## 21.2. Scope

All DHI information is categorized into five main classifications:

- DHI Public
- DHI Confidential
- Third Party Confidential
- Third Party Confidential Data
- Personally Identifiable Information (PII)

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

DHI Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of the company.

Other data considered as DHI Confidential information is confidential information belonging or pertaining to another corporation that has been entrusted to DHI by

that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into DHI's network to support our operations.

Third Party Confidential Information is information designated as confidential by a third party (vendor or customer) and entrusted to DHI. DHI will treat Third Party Confidential Information with the same standards as DHI Confidential Information.

Third Party Confidential Data is data designated as confidential by a third party (vendor or customer) and entrusted to DHI for use in DHI's production process.

DHI personnel are encouraged to use common sense judgment in securing DHI Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

## 21.3. Policy

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

## 21.4. DHI Public

Information Covered: General corporate information; some personnel and technical information.

There are no marking guidelines for this information in hardcopy or electronic form. However, all internal documents, even those with no marking present, should be considered confidential, unless expressly determined to be DHI Public information by an DHI employee with authority to do so.

- **Access** DHI employees, contractors, people with a business need to know.
- **Distribution within DHI** Standard interoffice mail, approved electronic mail and electronic file transmission methods.
- **Distribution outside of DHI internal mail** U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
- **Electronic distribution** No restrictions except that it be sent to only approved recipients.
- **Disposal/Destruction** Deposit outdated paper information in specially marked disposal bins on DHI premises; electronic data should be expunged/cleared periodically or when no longer needed. Reliably erase or physically destroy media.
- **Penalty for deliberate or inadvertent disclosure** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

## 21.5. DHI Confidential:

Information Covered: Business, financial, technical, and most personnel information, trade secrets & marketing, operational, personnel, financial, source code, and technical information integral to the success of our company

Note: all such documents must be accompanied with a red colored cover sheet, marked "DHI Confidential." In addition, every page of a confidential document must be marked "Confidential".

- **Access** Only those individuals (DHI employees and non-employees) designated with approved access and signed non-disclosure agreements.
- **Distribution within DHI** Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
- **Distribution outside of DHI internal mail** Delivered direct; signature required; approved private carriers and only after receipt of fully executed Non-Disclosure Agreement.
- **Electronic distribution** No restrictions to approved recipients (subject to receipt of fully executed Non-Disclosure Agreement) within DHI, but it is highly recommended that all information be strongly encrypted.
- **Storage** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer. Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- **Disposal/Destruction** Strongly Encouraged: In specially marked disposal bins on DHI premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media as per the DHI's Media Destruction Policy.
- **Penalty for deliberate or inadvertent disclosure** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

## 21.6. Third Party Confidential Information

DHI Will treat Third Party Confidential Information with the same standards as DHI Confidential Information.

## 21.7. Third Party Confidential Data

Third party data entrusted to DHI must adhere to the following standards:

- **Access** Only those individuals (DHI employees and non-employees) designated with approved access and signed non-disclosure agreements.
- **Distribution within DHI** Data must be shared with only those individuals who have direct responsibility for processing or consuming third party data.

- **Electronic distribution** All third party data must be encrypted prior to transmission over public networks using the InfoSec Encryption Standards Policy.
- **Wireless transmission** All third party data transmitted over a wireless network must be encrypted using Wi-Fi Protected Access (WPA), a VPN, or 128-bit SSL. WEP encryption of wireless connections is not allowed.
- **Personal Identifier Scrubbing** Where required by law or contract, DHI must render sensitive customer data unreadable anywhere it is stored, (including data on portable media, devices, mobile computers, smartphones, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
    - One-way hashes (hashed indexes) such as SHA-1
    - Truncation
    - Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedure
- **Storage** Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer. Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- **Disposal/Destruction** Strongly Encouraged: In specially marked disposal bins on DHI premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media as per the DHI's Media Destruction Policy.
- **Penalty for deliberate or inadvertent disclosure** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

## 21.8. Personally Identifiable Information (PII):

Information Covered: Uniquely identifying information about an individual. This information includes Driver's License Number, Social Security Number

Note: All files containing unencrypted PII must reside ONLY within the Lab Environment. No PII is to ever be accessible outside of the Lab.

- **Access** Only those individuals (DHI employees ONLY) designated with approved access and signed non-disclosure agreements.
- **Distribution within DHI** Unencrypted PII never leaves the Lab Environment.
- **Distribution outside of DHI internal mail** Delivered direct; signature required; approved private carriers and only after receipt of fully executed Non-Disclosure Agreement. Information is always encrypted for delivery
- **Electronic distribution** Distribution only to the individual who sent DHI the PII. (subject to receipt of fully executed Non-Disclosure Agreement). All information MUST be strongly encrypted.

- **Storage** Information is stored at rest encrypted and only accessible from the Lab environment.
- **Disposal/Destruction** Strongly Encouraged: In specially marked disposal bins on DHI premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media as per the DHI's Media Destruction Policy.
- **Penalty for deliberate or inadvertent disclosure** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

## 21.9. Definitions

### 21.9.1. Appropriate measures

To minimize risk to DHI from an outside business connection, DHI computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access DHI corporate information, the amount of information at risk is minimized.

### 21.9.2. Configuration of DHI-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

### 21.9.3. Delivered Direct; Signature Required

Do not leave in interoffice mail slot; call the mailroom for special pick-up of mail.

### 21.9.4. Approved Electronic File Transmission Methods

Includes supported SFTP clients and SSL Web browsers.

### 21.9.5. Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

### 21.9.6. Approved Electronic Mail

Includes all mail systems supported by the IT Support Team.

### 21.9.7. Approved Encrypted email and files

Techniques include the use of DES, PGP, 3DES, AES, Blowfish, Psypher, PGP, GPG, DES encryption is available via many different public domain packages on all

platforms. PGP use within DHI is done via a license. Please contact the appropriate support organization if you require a license.

### 21.9.8. Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

### 21.9.9. Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

### 21.9.10. 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.

### 21.9.11. 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 DHI.

### 21.9.12. Encryption

Secure DHI 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.

### 21.9.13. One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to DHI’s internal network over the Internet. Contact your support organization for more information on how to set this up.

### 21.9.14. Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make

arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

### 21.9.15. Private Link

A Private Link is an electronic communications path that DHI has control over its entire distance. For example, all DHI networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. ISDN lines or use of VPN clients from employee's homes are a private link. DHI also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies that DHI has established private links include all announced acquisitions and some short-term temporary links.

# 22. Internal Lab Security Policy

## 22.1. Purpose

This policy establishes information security requirements for DHI labs to ensure that DHI confidential information and technologies are not compromised, and that production services and other DHI interests are protected from lab activities.

## 22.2. Scope

This policy applies to all internally connected labs, DHI employees and third parties who access DHI's labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. Air-gapped labs are exempt from this policy.

## 22.3. Policy

### 22.3.1. Ownership Responsibilities

1. Lab owning groups are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with INFSEC and IT Management. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard DHI from security vulnerabilities.
3. Lab managers are responsible for the lab's compliance with all DHI security policies. The following are particularly important: Password Policy for networking devices and hosts, Wireless Communication Policy, Anti-Virus Policy, Remote Access Policy, and Employee and Contractor Access Policies.
4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
5. The network support group must maintain a firewall device between the corporate production network and all lab equipment.
6. The network support group and/or INFOSEC reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

7. The network support group must record all lab IP addresses, which are routed within DHI networks, in Enterprise Address Management database along with current contact information for that lab.

8. Any lab that wants to add an external connection must provide a diagram and documentation to INFOSEC with business justification, the equipment, and the IP address space information. INFOSEC will review for security concerns and must approve before such connections are implemented.
9. All user passwords must comply with DHI's Password Policy. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains DHI proprietary information, group account passwords must be changed within three (3) days following a change in group membership.
10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities.
11. INFOSEC will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

## 22.4. General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network support group maintained firewall. All lab network devices must not cross-connect the lab and production networks.
2. Original firewall configurations and any changes thereto must be reviewed and approved by INFOSEC. INFOSEC may require security improvements as needed.
3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-DHI networks. These activities must be restricted within the lab.
4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.
5. INFOSEC reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.
6. Lab owned gateway devices are required to comply with all DHI product security advisories and must authenticate against the Corporate Authentication servers.
7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in

accordance with DHI's Password Policy. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-DHI personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no DHI confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by INFOSEC.
9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must be hardened and given highly restricted access if they are located in open areas.
10. All lab external connection requests must be reviewed and approved by INFOSEC. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.
11. All labs networks with external connections must not be connected to DHI corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from INFOSEC is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

## 22.5. Definitions

- **Internal** A lab that is within DHI's corporate firewall and connected to DHI's corporate production network
- **Network support group** Any INFOSEC approved DHI support organization that manages the networking of non-lab networks.
- **Lab Manager** The individual responsible for all lab activities and personnel
- **Lab** A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
- **External Connections (also known as DMZ)** External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
- **Lab Owned Gateway Device** A lab owned gateway device is the lab device that connects the lab network to the rest of DHI network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by INFOSEC.
- **Traffic** Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
- **Firewall** A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by INFOSEC.
- **Extranet** Connections between third parties that require access to connections non-public DHI resources, as defined in INFOSEC's Extranet policy (link).

- **DMZ (De-Militarized Zone)** This network structure describes the network that exists outside of primary corporate firewalls, but are still under DHI administrative control.

# 23. Internet DMZ Equipment Policy

## 23.1. Purpose

The purpose of this policy is to define standards to be met by all equipment owned and/or operated by DHI located outside DHI's corporate Internet firewalls. These standards are designed to minimize the potential exposure to DHI from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of DHI resources.

Devices that are Internet facing and outside the DHI firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

## 23.2. Scope

All equipment or devices deployed in a DMZ owned and/or operated by DHI (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by DHI, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "DHI.com" domain or appears to be owned by DHI.

All new equipment that falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from INFOSEC. All existing and future equipment deployed on DHI's un-trusted networks must comply with this policy.

## 23.3. Policy

### 23.3.1. Ownership and Responsibilities

Operational support groups approved by INFOSEC for DMZ system, application, and/or network management must administer equipment and applications within the scope of this policy.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.

    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the corporate wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of INFOSEC upon demand, per the Audit Policy.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify compliance with this policy, INFOSEC will periodically audit DMZ equipment per the Audit Policy.

## 23.4. General Configuration Policy

All equipment must comply with the following configuration policy:

- INFOSEC as part of the pre-deployment review phase must approve hardware, operating systems, services and applications.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All interactive applications must be reviewed for security concerns by INFOSEC before they are placed into the DMZ. This is especially true for any e-commerce applications.
- All patches/hot-fixes recommended by the equipment vendor and INFOSEC must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by INFOSEC.
- Access control lists must restrict services and applications not for general access.
- Insecure services or protocols (as determined by INFOSEC) must be replaced with more secure equivalents whenever such exist.
- 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. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.

- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to INFOSEC-approved logs. Security-related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- INFOSEC will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

## 23.5. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- INFOSEC must be invited to perform system/application audits prior to the deployment of new services.
- INFOSEC must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

## 23.6. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

## 23.7. Definitions

- **DMZ (de-militarized zone):** Any un-trusted network connected to, but separated from, DHI's corporate network by a firewall, used for external (Internet/partner, etc.) access from within DHI, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.
- **Secure Channel:** Out-of-band console management or channels using strong encryption according to the Acceptable Encryption Policy. Non-encrypted channels must use strong user authentication (one-time passwords).
- **Un-Trusted Network:** Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks or the Internet), or anything else identified as a potential threat to those resources.

# 24. Laptop Security Policy

## 24.1. Purpose

To document methods for DHI employees to employ in order to secure their laptops from theft or unauthorized access.

## 24.2. Scope

These tips are suggested for all DHI employees who use laptop computers.

## 24.3. Policy

Always use an anti-theft device. Portable locking device and motion sensor alarms are available from the INFOSEC group.

Never leave your laptop in open view in your car. Lock it in your trunk.

If possible, carry your laptop in an unassuming, well padded bag. This avoids the unwanted attention a traditional laptop bag or fancy leather briefcase can generate.

Never leave your laptop unattended in a public place, including your office (absent an anti-theft device). Secure it to your desk at all times, or lock it in a drawer, or "lock-box" even if you leave for a moment. Never leave it unattended anywhere, including your home.

Never put your laptop on the airport security x-ray machine belt before you have a clear path to the end of the belt.

Back up all irreplaceable information daily. Remember, it's not just the loss of the laptop...what about all the hard work and important information that could be lost or stolen. Backing up irreplaceable data is easily achieved by placing critical documents and files into “My Documents”.

Don't forget to secure all other products associated with your laptop: batteries, power cords, cables, external drives, LCD projectors, etc...

When traveling, you can also use neon tape or stripes on your laptop's bag for quick identification in a crowd. If you use an easily identifiable bag, thieves will be discouraged. A lime-green stripe makes your bag easier to identify than all those black bags used by business travelers.

Before you leave on any trip, record your laptop's serial number in two places. Keep one separated from your laptop and keep the other at home. If your laptop is stolen, you can give the serial number to the authorities to aid in the search.

# 25. Mass Storage Device Policy

## 25.1. Purpose

The purpose of this policy is to provide guidance that limits the use of portable USB/Firewire devices (such as mp3 players, thumb drives, and portable disk enclosures) within the DHI computing environment.

## 25.2. Scope

This policy applies to all DHI employees and affiliates.

## 25.3. Policy

No unauthorized USB or FireWire (IEEE 1394) devices are to be connected to DHI systems. Authorization for mass storage devices must be obtained from InfoSec or the VP Operations. Under no circumstances are USB devices to be used to store confidential data without the express written permission of InfoSec or the VP Operations. All data on removable media must be encrypted.

## 25.4. Definitions

- **Firewire** A serial bus interface standard allowing high-speed connections between devices.
- **USB** Universal Serial Bus - a serial bus standard for connecting devices.

# 26. Media and Data Destruction Policy

## 26.1. Purpose

The purpose of this policy is to define standards for the destruction of old or unnecessary data on media. These standards are designed to minimize the potential exposure to DHI from damages that may result from the accidental release of DHI data. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical DHI internal systems, etc.

## 26.2. Scope

This policy applies to all DHI employees, contractors, vendors and agents who work within the DHI environment.

## 26.3. Policy

### 26.3.1. General

It is the responsibility of DHI employees, contractors, vendors and agents to ensure that all media that contains data that is no longer needed is disposed of in a secure manner. Such media may include (but is not limited to) CD-Roms, DVDs, diskettes, magnetic tape, hard disks, and other magnetic media. Additionally, any data devices that are to be returned to vendors or third parties (i.e., hard disks), must have all DHI data securely removed from it before being returned. A shredder box (as described herein) is available on company premises for such destruction.

### 26.3.2. Requirements

1. All non-disposable media (such as a hard drives) that are to leave the DHI environment must have all DHI's data removed from them before they leave the premises. Said data removal must be done according to current industry specifications. Currently, this consists of five-time overwrites via use of shredding software approved by INFOSEC. Simple file deletion is not acceptable, since such data can be recovered with ease.
2. As required by 3rd Parties data on physical media will be shredded.
3. Data on internal DHI systems that is no longer needed may be deleted without scrubbing, as long as those systems remain in use within their current environment. Any systems containing sensitive data must be scrubbed with approved software before they are released into the general-use desktop pool.

### 26.3.3. Definitions

- **Shredding** The process of rewriting sectors on a hard disk several times to render the data on said disk unrecoverable.

- **Scrubbed** A system that has had its data “shredded” as above is considered to be “scrubbed”.
- **3rd Parties** Scrubbing of physical media as specified by either vendor or a customer.

# 27. Password Policy

## 27.1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of DHI's entire corporate network. As such, all DHI employees (including contractors and vendors with access to DHI systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## 27.2. Purpose

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

## 27.3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DHI facility, has access to the DHI network, or stores any non-public DHI information. Additionally, this policy's scope is extended to include anyone who has access to customer equipment/systems requiring passwords (i.e. customer FTP servers).

## 27.4. Policy

### 27.4.1. General

- All users must have a unique username and password.
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every thirty (30) days.
- All production system-level passwords must be part of the INFOSEC administered global password management database.
- Passwords must not be changed more than once with a 24 hour period.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every ninety (60) days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user. On all linux/unix systems, all logins to privileged accounts must be through a non-privileged account, except at the root console.
- SSH root logins must be disabled whenever possible (i.e. where ILO is in place).
- Passwords must not be inserted into email messages or other forms of electronic communication.

- All user-level and system-level passwords must conform to the guidelines described below.
- All systems are to be configured to require the user to enter a password/passphrase before they can access said system. For example, if a user accesses 5 systems, the user must be prompted for 5 passwords/passphrases. The password/passphrase can be substituted by biometric authentication where possible.
- All Systems are to be configured to lock out the account after three failed password attempts for a minimum of 60 minutes.

### 27.4.2. General Password Construction Guidelines

Passwords are used for various purposes at DHI. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "DHI", "cherryhill", or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

**NOTE: Do not use either of these examples as passwords!**

### 27.4.3. Password Protection Standards

Do not use the same password for DHI accounts as for other non-DHI access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various DHI access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

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

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't send a password in an email message with a username
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don’t use the “remember password” option offered by most browsers
- Don’t write or store the password in plain text

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

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

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

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

### 27.4.4. Application Development Standards

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

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.

- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
- Vendor passwords must only be maintained as long as necessary for the vendor to complete his/her work.

### 27.4.5. Use of Passwords and Passphrases for Remote Access Users

Access to the DHI networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase. SSH root logins must be disabled wherever possible.

### 27.4.6. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnTheI95Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

### 27.4.7. Password Creation, Maintenance, and Deletion

It will be the responsibility of the employee’s departmental manager to determine the access requirements for each system. (Building Access, Email, TFS, etc.). Upon creation of an account for an employee or contractor the account name, and account type will be communicated to Human Resources. Upon termination Human Resources will be responsible that the appropriate account custodian removes the employees access from the system.

## 27.5. Definitions

- **Application Administration Account** Any account that is for the administration of an application

# 28. Peer to Peer Policy

## 28.1. Purpose

The purpose of this policy is to provide guidance for DHI employees regarding the use of peer to peer software.

## 28.2. Scope

This policy applies to all DHI employees and affiliates.

## 28.3. Policy

In order to ensure our compliance with contractual agreements and industry best practices, and to assist us in remaining compliant with copyright laws, DHI forbids the use of peer to peer software to regular employees. Only employees within InfoSec and Operations are permitted to use peer to peer technology, and may only use said software to download public domain software. All downloaded software must be scanned for viruses before being deployed in the DHI network environment. Peer to peer software is not to be used to download copyrighted material that DHI does not have a license for.

## 28.4. Definitions

- **Peer to Peer** A sharing and delivery of user specified files among groups of people who are logged on to a file sharing network. Napster, BitTorrent, and Emule are examples of peer to peer networks/clients.

# 29. Personal Use Policy

## 29.1. Purpose

To explain the conditions under which non-official use of company computing resources and services is permitted.

## 29.2. Scope

This policy applies to all full and part time employees and contractors with DHI.

## 29.3. Policy

### *Computer, email and internet usage*

- Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role
- All Internet data that is composed, transmitted and/or received by DHI computer systems is considered to belong to DHI and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
- The equipment, services and technology used to access the Internet are the property of DHI and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by DHI if they are deemed to be harmful and/or not productive to business
- The installation of software such as instant messaging technology is strictly prohibited

### *Unacceptable use of the internet by employees includes, but is not limited to:*

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via DHI email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization

- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification

All terms and conditions as stated in this document are applicable to all users of DHI network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by DHI.

# 30. Physical Building Access Policy

## 30.1. Purpose

The objective of the Physical Building Access Policy is to provide a comprehensive, dependable and cost-effective security access control and security system solution for DHI, its employees and its assets. The system will consist of an integrated pairing of the traditional mechanical locking or keyed system, with a newly selected computer based access control system that will allow for use of primarily card access control, and will set a standard for security systems within DHI.

## 30.2. Scope

The scope of this document applies to the physical building located at 1 Keystone Avenue and to any ancillary buildings used by DHI

## 30.3. Policy

### 30.3.1. General

- Effective February 1, 2014, Employees are required to immediately report to the security administrator forgotten or lost security access cards. Security administrator is required to immediately deactivate the security access card.
- All physical security systems must comply with applicable all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Human Resources are responsible for issuing building access cards/codes to new employees and for removing those codes upon termination of employment.
- Each individual that is granted access rights to the facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to Human Resources. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to Human Resources.
- Cards and/or keys must not have identifying information other than a return mail address.
- All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- All visitors must be escorted by a Drivers History employee at all times.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.

- Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Human Resources must remove the card and/or key access rights of individuals that change roles within DHI or are separated from their relationship with DHI.

### 30.3.2. Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to civil, and criminal prosecution.

# 31. Remote Access Policy

## 31.1. Purpose

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

## 31.2. Scope

This policy applies to all DHI employees, contractors, vendors and agents with an DHI-owned or personally owned computer or workstation used to connect to the DHI network. This policy applies to remote access connections used to do work on behalf of DHI, 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.

## 31.3. Policy

### 31.3.1. General

1. It is the responsibility of DHI employees, contractors, vendors and agents with remote access privileges to DHI's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DHI.
2. General access to the Internet for recreational use by immediate household members through the DHI Network on personal computers is not permitted. The DHI employee bears responsibility for the consequences should access be gained by a household member.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of DHI's network:
    - Acceptable Encryption Policy
    - Wireless Communications Policy
    - Acceptable Use Policy

- Effective February 1, 2014, remote access from non-company owned assets is strictly prohibited.
- Effective February 1, 2014, remote access is only permitted with company owned devices
- Effective February 1, 2014, all remote access requires two-factor authentication.

### 31.3.2. Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any DHI employee provide his or her login or email password to anyone, not even family members.
3. DHI employees and contractors with remote access privileges must ensure that their DHI-owned or personal computer or workstation, which is remotely connected to DHI's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Routers for dedicated ISDN lines configured for access to the DHI network must meet minimum authentication requirements of CHAP.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Frame Relay must meet minimum authentication requirements of DLCI standards. The Network Administrator must approve non-standard hardware configurations, and INFOSEC must approve security configurations for access to hardware.
7. All hosts that are connected to DHI internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.
8. Personal equipment that is used to connect to DHI's networks must meet the requirements of DHI-owned equipment for remote access.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the DHI production network must obtain prior approval from the Network Administrator and INFOSEC.

## 31.4. Definitions

- **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. DLCI (Data Link Connection Identifier) 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 DHI-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into DHI 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 DHI's corporate network through a non-DHI controlled network, device, or medium.
- **Split-tunneling** Simultaneous direct access to a non-DHI network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DHI'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.

# 32. Risk Assessment Policy

## 32.1. Purpose

To empower INFOSEC to perform periodic information security and privacy risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

## 32.2. Scope

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

## 32.3. Policy

The execution, development and implementation of remediation programs is the joint responsibility of INFOSEC and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the INFOSEC Risk Assessment Team in the development of a remediation plan. RAs should be performed semi-annually.

## 32.4. Definitions

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

# 33. Router Security Policy

## 33.1. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of DHI.

## 33.2. Scope

All routers and switches connected to DHI production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the Internet DMZ Equipment Policy.

## 33.3. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement."

## 33.4. Definitions

**Production Network** The "production network" is the network used in the daily business of DHI. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to DHI employees or impact their ability to do work.

**Lab Network** A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to DHI nor affect the production network.

# 34. Server Security Policy

## 34.1. Purpose

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

## 34.2. Scope

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

This policy is specifically for equipment on the internal DHI network. For secure configuration of equipment external to DHI on the DMZ, refer to the Internet DMZ Equipment Policy.

## 34.3. Policy

### 34.3.1. Ownership and Responsibilities

An operational support group that is responsible for system administration must own all internal servers deployed at DHI. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by INFOSEC. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by INFOSEC.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

### 34.3.2. General Configuration Guidelines

- Operating System configuration should be in accordance with approved INFOSEC guidelines.
- Services and applications that will not be used must be disabled where practical.

- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Only systems that require CCB approval may be excluded from automatic system updates. Those exempted systems must implement said patches within 2 weeks of them being determined as "stable", or within 48 hours of being approved by the CCB (whichever comes first).
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

### 34.3.3. Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs would be kept online for a minimum of one week.
    - Daily incremental tape backups will be retained for at least one month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to INFOSEC, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

### 34.3.4. Compliance

- Audits will be performed on a regular basis by authorized organizations within DHI.

- The internal audit group or INFOSEC, in accordance with the Audit Policy, will manage audits. INFOSEC will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

### 34.3.5. Definitions

- **DMZ** De-militarized Zone. A network segment external to the corporate production network.
- **Server** For purposes of this policy, a Server is defined as an internal DHI Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

# 35. System Hardening Policy

## 35.1. Overview

Hardening is the process of securing a system by reducing its surface of vulnerability. By the nature of operation, the more functions a system performs, the larger the vulnerability surface.

Most systems perform a limited number of functions. It is possible to reduce the number of possible vectors of attack by the removal of any software, user accounts or services that are not related and required by the planned system functions.

System hardening is a vendor specific process, as different system vendors install different elements in the default install process.

The possibility of a successful attack can be further reduced by obfuscation. By making it difficult for a potential attacker to identify the system being attacked the attack can not easily exploit known weaknesses

## 35.2. Scope

This policy applies to all components of the information technology infrastructure

and includes:

- Computers
- Servers
- Application Software
- Peripherals
- Routers and switches
- Databases
- Telephone Systems

All staff within the IT Department must understand and use this policy. IT staff are responsible for ensuring that the IT infrastructure is hardened and that any subsequent changes to systems do not affect the hardening of systems.

## 35.3. Policy

All new systems will undergo the following hardening process.

- Install system
- Remove unnecessary software
- Disable or remove unnecessary usernames
- Disable or remove unnecessary services
- Patch system
- Perform vulnerability scan
- Vulnerabilities

- Install anti-virus and anti-malware
- Configure firewall
- Install System

# 36. Teleworking Policy

## 36.1. Purpose

The purpose of Teleworking is to provide a framework for employees who work from remote locations.

## 36.2. Scope

This policy applies to employees who work primarily or exclusively from a remote location outside of the primary DHI office location.

## 36.3. Policy

Teleworking permits the DHI to designate employees who will work at alternate work locations for all or part of the workweek in order to promote general work efficiencies. To the greatest extent practicable, the policies and procedures that normally apply to the central workplace shall remain the same for the teleworking employee. Some positions have job responsibilities or functions that do not lend themselves to teleworking. Therefore, teleworking is not an option for all employees.

Once a department or unit determines that a teleworking arrangement would be beneficial in improving general work efficiencies, a written request must be forwarded to the appropriate unit head/director for review and approval. This request shall include the responsibilities of both DHI and the employee. Each participant in a teleworking arrangement must sign the Teleworking Agreement, the Teleworker Assignment, the Remote Workspace Self-Certification Checklist, and shall comply with the policy provisions below:

### 36.3.1. Compensation and Benefits

The employee's compensation, benefits, work status and work responsibilities will not change due to teleworking. The amount of time the employee is expected to work per day or pay period will not change as a result of participation in the Teleworking Program. Job responsibilities and work output will continue to follow the standards as set forth by DHI.

### 36.3.2. Safety and Ergonomics

In a manner consistent with the DHI Safety and Health Policy, employees and supervisors will work together to make safety an integral part of the teleworking process. The employee is responsible for maintaining the telework site in a manner free from health or safety hazards and for notifying his/her supervisor immediately of any unsafe conditions in the designated workspace, or of any pain which accompanies computer use or teleworking activities. It is very important that early warning signs of pain or discomfort are reported before an actual injury/illness occurs. It is the responsibility of the supervisor to educate the employee about potential hazards involved in the teleworking process, follow up on reports of pain or injury to improve the workspace, and take steps to mitigate or eliminate these hazards. All identified health or safety issues must be abated in a timely manner.

### 36.3.3. Workers' Compensation

The employee will be covered by workers' compensation for job-related injuries that occur in the course and scope of employment while teleworking. In cases where the home and the designated workplace are the same, workers' compensation will not apply to non-job related injures that might occur at the telework site.

### 36.3.4. Materials, Equipment, and Security

Based on the type of work to be performed, DHI may provide computer hardware, computer software, phone lines, email, voice mail, connectivity to host applications, Internet connectivity and other applicable equipment as deemed necessary by the employee's supervisor. Restricted access materials must not be compromised in any way and teleworking employees must take all precautions necessary to secure these materials. DHI assumes no responsibility for the employee's personal property.

### 36.3.5. Work Hours

Employees are expected to perform their work during designated work hours and not engage in activities that are not work-related.

DHI may terminate the Teleworking Agreement at its discretion.

# 37. Third Party Security Incident Reporting

## 37.1. Purpose

The purpose of Third Party Security Incident Reporting is to provide a framework to communicate to invested third parties when a security incident has occurred involving their data.

## 37.2. Scope

This policy applies to all data in possession of DHI that is the property or subject to licensing requirements of a third party

## 37.3. Policy

Upon execution of a third party contract requiring third party security incident reporting DHI's Corporate Counsel will work with the Information Security Lead Security Administrator to internally define Restricted Data.

The Corporate Counsel will also be responsible for assembling a 3rd party incident response contact list.

The Lead Security Administrator will be responsible for internally identifying and tracking Restricted Data upon a security breach.

It is the responsibility of ALL employees to IMMEDIATELY notify InfoSec or the CTO when a Third Party Security Incident has occurred.

Once a breach has occurred Corporate Counsel will be responsible for all 3rd party communications. Unless such disclosure is mandated by applicable law or regulation, DHI in its sole discretion will determine whether to provide notification to customers, employees, agents or government authorities concerning a breach or potential breach of security or any other type or form of Security Incident.

## 37.4. Definition

- **Security Incident** Unauthorized Access of Third Party Restricted Data including, but not limited to disclosure, theft or manipulation of information that has the potential to cause harm to a Third Party systems or Third Party information
- **Restricted Data** Data that is not wholly owned by DHI and is contractually restricted in use or movement.
- **Third Party** A vendor who provides information to DHI or a customer who provides confidential information to DHI for use in DHI's products.

# 38. Vendor Management Audit Policy

## 38.1. Purpose

This policy outlines the audit requirements for all DHI vendors that support any areas of the DHI enterprise that store, have access to, or might otherwise see sensitive information, and vendors that provide mission critical production support.

## 38.2. Scope

This policy covers the inclusion of vendors in DHI's risk assessment program and the requirement to include "right to audit" language in vendor contract meeting the above requirements stated in 38.1.

## 38.3. Policy

- Vendors meeting the above criteria in section 38.1 will be included in DHI's risk assessment program and process.
- All new vendors, effective June 2014, meeting the above criteria will have "right to audit" language in the contracts.

Sample contract language below subject to final review and approval of DHI general counsel.

**Audits and Inspections**

Company agrees that upon the request of DHI, Company shall permit and participate (at no extra cost to DHI) in reasonable audit(s) of Company's security policies, procedures and controls, which audit(s) may occur with 1(one) week advance notice to Company and include on-site review(s) at Company locations.

# 39. Vulnerability Detection and Security Patch Standards Policy

## 39.1. Purpose

The purpose of this policy is to establish and maintain standard operating procedures to detect vulnerabilities in the network, and to implement patches for any discovered vulnerabilities in a timely manner.

## 39.2. Scope

This policy applies to all systems within DHI.

## 39.3. Policy

In order to ensure the most secure computing environment as well as to comply with various regulations, DHI will routinely scan our internal and external network routinely to discover any vulnerabilities.

- InfoSec shall monitor any major security bulletin boards/discussion groups/mailing lists (such as BugTraq, Full Disclosure, ISN) to identify any new or developing vulnerabilities in applications currently in use within the DHI network.
- InfoSec shall maintain Host Based Intrusion Detection on all production servers and servers housing DHI Confidential Information or Third Party Confidential Data.
- InfoSec shall scan the internal and external networks on a recurring basis (a minimum of once every quarter) to identify any possible vulnerabilities. Said scans do not have to have DOS probes included.
- InfoSec shall routinely scan the premises for unauthorized wireless access points.
- Any identified problems shall be forwarded to the network manager within 48 hours.
- InfoSec shall routinely check the Microsoft SUS server for updated patches. All patches must be implemented within 14 days of release.
- InfoSec shall routinely check the server image distributions to ensure all current patches are in place.
- Only InfoSec is authorized to run vulnerability scans against our own network. Written permission must be obtained from the VP Operations for others to perform such scans. Any such permission must be forwarded to InfoSec in order for them to disregard and notate any such scans from their logs.
- Newly discovered vulnerabilities will be assessed for potential changes to the DHI InfoSec Policy.

# 40. Wireless Communication Policy

## 40.1. Purpose

This policy prohibits access to DHI networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by INFOSEC are approved for connectivity to DHI's networks. The INFOSEC group must be informed of any wireless network before it is installed. Due to their nature, wireless networks are not preferred and will rarely be authorized.

## 40.2. Scope

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

## 40.3. Policy

No wireless networks are to be implemented unless all traffic over them is encrypted via a VPN protocol such as IPSEC. Additionally, wireless implementations must:

- Maintain point to point hardware encryption of at least 128 bits.
- Maintain a hardware address that can be registered and tracked, i.e., a MAC address.
- Support strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

## 40.4. Definitions

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

# 41. Mobile Computing Policy

## 41.1. Purpose

The purpose of this policy is to outline appropriate and secure use of mobile computing devices.

## 41.2. Scope

This policy applies to all DHI employees that have been approved to use mobile devices for company sponsored use and access to corporate email.

## 41.3. Policy

- Any use of corporate sponsored mobile devices requires approval from the CIO. All devices must be encrypted, password protected and subject to remote wipe control. Any lost or stolen devices must be reported to the CIO or email administrator within an hour of the event.
- Only corporate email and non-customer centric files are allowed on mobile devices. It is absolutely prohibited to store any client-related data or information on mobile devices. Employee's found to be storing any unauthorized information on mobile devices will be subject to discipline up to and including termination.
- Mobile devices will be fully wiped upon employee termination.