



# DATAMATION

## Information Security Manual

### Table of Contents

### *Information Security Policy and Standards*

#### **Company Information Security Policy**

---

Purpose	Policy-1
Scope	Policy-1
Policy	Policy-1
Enforcement	Policy-1
Compliance	Policy-1
Responsibilities	Policy-2
Policy Statements	Policy-2
Exceptions	Policy-5
Related Policies	Policy-5
Standards	Policy-5
Revisions	Policy-5
Distribution of this Manual	Policy-5

#### **Chapter 1: User Accountability**

Introduction	1-1
Policy Statement	1-1
Standards	1-1
User Accountability	1-1
Effective Passwords	1-2
Ineffective Passwords	1-2
Managing Multiple Passwords	1-3
Responsibilities	1-3
References	1-4

#### **Chapter 2: Electronic Mail**

Introduction	2-1
Policy Statement	2-1
Standards	2-1
Management's Right to Access Information	2-1
Message Content	2-1
Message Integrity and Disclosure	2-2
Safeguards of E-Mail Systems	2-2

---

Internet E-Mail	2-2
Other E-Mail Considerations	2-3
Responsibilities	2-3
References	2-4
<b>Chapter 3: Internet Access</b>	
Introduction	3-1
Policy Statement	3-1
Standards	3-1
Acceptable Use	3-1
Public Representation	3-3
Infrastructure Monitoring	3-3
Requesting Internet Access	3-4
Internet Gateway Locations	3-4
Internet Gateway Requests	3-4
Responsibilities	3-5
References	3-5
<b>Chapter 4: Software Licensing and Use</b>	
Introduction	4-1
Policy Statement	4-1
Standards	4-1
Software Use	4-1
Software Licensing	4-1
Appropriate Software	4-3
Software/License Monitoring	4-3
Responsibilities	4-4
<b>Chapter 5: Virus Protection</b>	
Introduction	5-1
Policy Statement	5-1
Standards	5-1
Symptoms and Indicators	5-1
Prevention	5-1
Responsibilities	5-3
<b>Chapter 6: Access Controls</b>	
Introduction	6-1
Policy Statement	6-1
Standards	6-1
Acknowledgment of Non-Disclosure Agreement	6-1
Identification and Authentication of Users	6-1
Data and Software	6-4
Responsibilities	6-4
References	6-5
<b>Chapter 7: System and Application Controls</b>	
Introduction	7-1
Policy Statement	7-1

Standards	7-1
Segregation of Duties and Key Dependencies	7-1
Change Control	7-1
Internet Application Development	7-2
Operating Systems and Application Patch Updates	7-3
Documentation Standards	7-3
Internal Application Security	7-4
Responsibilities	7-4
References	7-5
<b>Chapter 8: Physical and Environmental Controls</b>	
Introduction	8-1
Policy Statement	8-1
Standards	8-1
Fire Protection	8-2
Access and Security Protection	8-2
General Environment Protection	8-3
Responsibilities	8-4
<b>Chapter 9: Telecommunications</b>	
Introduction	9-1
Policy Statement	9-1
Standards	9-1
Voice Communications	9-1
Telephone Maintenance	9-1
Voicemail Access	9-2
PBX Access	9-3
Telephone Cost Management	9-4
Telecommunications User Management	9-5
Long Distance Telephone Charges	9-6
Problem Resolution / Disaster Recovery	9-6
Responsibilities	9-6
References	9-7
<b>Chapter 10: Information Classification</b>	
Introduction	10-1
Policy Statement	10-1
Standards	10-1
Sensitive Applications or Data	10-1
Information Owner, Custodian, Users, and Managers	10-2
Controlling Access to Sensitive Computer Information	10-3
Information and the Internet	10-3
Information Disposal	10-3
Responsibilities	10-4
<b>Chapter 11: Personal Data Protection</b>	
Introduction	11-1
Policy Statement	11-1
Standards	11-1

Collection Limitations	11-1
Data Quality	11-1
Purpose Specification	11-1
Use Limitation	11-1
Security Safeguards	11-1
Openness	11-1
Individual Participation	11-2
Accountability	11-2
Relevant Laws	11-2
<b>Chapter 12: Segregation of Duties</b>	
Introduction	12-1
Policy Statement	12-1
Standards	12-1
Segregation of Duties	12-1
Compensating Controls	12-1
Responsibilities	12-1
General Ledger	12-3
Accounts Receivable	12-4
Accounts Payable	12-5
Payroll and Human Resources	12-6
Materials Management	12-7
Information Technology	12-8
<b>Chapter 13: Disaster Recovery</b>	
Introduction	13-1
Policy Statement	13-1
Standards	13-1
Objective	13-1
Responsibilities	13-2
The Disaster Recovery Plan	13-2
Backup/Data Recovery	13-3
Testing and Maintaining the Plan	13-4
Communication/Awareness/Distribution	13-5
Alternative Sites/Contingency Planning	13-5
Risk Analysis	13-5
Existing Systems	13-6
New Systems	13-6
<b>Chapter 14: Network Security</b>	
Introduction	14-1
Policy Statement	14-1
Standards	14-1
Configuring Networks	14-1
Managing and Monitoring	14-1
Connecting	14-2
Accessing Remotely	14-2
Third Party and Vendor Access	14-3
Compliance Statement	14-3

Wireless Networks	14-4
Network Services	14-4
Segregation of Network	14-5
Data Exchange and Encrypted Links	14-5
Modem Usage & Outbound Connections	14-5
Remote Control	14-6
Radio and Cellular	14-6
Shared File Systems	14-6
Logs for Externally Connected Systems	14-7
Unauthorized Access & Network Browsing	14-7
Changes to Networks	14-7
Installation of Communication Lines	14-7
New Business Networks	14-8
Disclosure of Systems Information	14-8
Security Tools	14-8
<b>Chapter 15: Gateway Standards</b>	
Introduction	15-1
Policy Statement	15-1
Standards	15-1
Hardware and Software	15-2
Management and Control	15-2
Monitoring	15-9
Training and Support	15-12
Virtual Private Networks	15-12
Third Party Connections	15-13
Exceptions	15-13
Compliance	15-13
Diagrams	15-14
<b>Appendix:</b>	
<b>Laptop PC Security</b>	Appendix
<b>Forms &amp; Other Documents:</b>	
Non-Disclosure Agreement	Form A
Company Information Security Handbook	Form B
Internet Policy Acknowledgement	Form C
Remote Access Policy and Acknowledgement	Form D
Security Awareness Policy Acknowledgement	Form E

# Company Information Security Policy

## PURPOSE

This Policy and its related Standards state the requirements for protecting information resources at Datamation Company. The Policies and Standards have been developed to control business risks and ensure the proper Datamation image is presented.

## SCOPE

This Policy applies to all Datamation employees, contractors, vendors and/or suppliers, temporary staff members, and joint venture companies as well as any other person or company who accesses Datamation's network resources. All information, regardless of the media on which it is stored, as well as automated systems used to store, process, and transmit information, are included under this Policy. The Policy includes all computer-related activity while using Company equipment, on Company facilities, or when accessing Company information.

In addition, this Policy applies to information resources that have been entrusted to Datamation by the Client or an entity outside the Company.

## POLICY

Information is a valuable asset to the Company. The preservation of its integrity, confidentiality, and availability is essential to the success of Datamation. Measures must be taken to protect information and information processing systems against unauthorized use, modification, disclosure, and destruction, whether accidental or intentional. The method used to protect information resources must be consistent with the value of those resources.

## ENFORCEMENT

Management, Information Security, and Internal Audit Services have the right and responsibility to monitor the use of Company information resources and compliance with Information Security Policies and Standards. Specifically, management is responsible for enforcing Policies and Standards while Internal Audit Services is responsible for evaluating compliance with Policies and Standards.

## COMPLIANCE

**Laws of individual states supersede the Information Security Policy and Standards.**

Any use of information resources other than to support Datamation's business objectives will be considered a violation of Policy. Violations or suspected violations of Policy and related Standards must be reported immediately to the Information Security Department. Failure to comply with Policy and related Standards may result in disciplinary action up to and including termination of employment or contractual relationships.

# Company Information Security Policy

Datamation , at its discretion, may also pursue civil remedies or criminal prosecution.

## **RESPONSIBILITIES**

The protection of Company information is a basic responsibility of all employees and service providers.

Management is responsible for the identification, classification, and protection of information resources within the scope of their authority. Management must assume ownership responsibilities of the information and/or applications.

Executive Management is responsible for approving and endorsing the Information Security Policy and supporting sub-policies.

Guidance, direction, and authority for information security activities are the responsibility of Datamation Information Security.

## **POLICY STATEMENTS**

### ***User Accountability***

Each user must have a unique user identification code and password to access Company computer systems. In addition, users are responsible and accountable for all actions performed under their user ID.

### ***Electronic Mail***

Company E-mail systems are to be used for business purposes only. Datamation treats all E-mail messages sent, received, and/or stored in its systems as Company records. Company E-mail systems **must not** be used to continue, distribute, or circulate **chain letters** or **inappropriate/offensive content**.

Datamation does not assure any personal right of privacy for any E-mail message or document transmitted through the use of Company equipment or systems. Datamation reserves the right to access all E-mail messages transmitted through Company equipment or systems, without prior notice, and to disclose the message to any person or entity that Datamation deems appropriate. Datamation retains the right to determine the acceptable use of its E-mail systems.

### ***Internet Access***

Authorized Internet users will behave in an ethical, legal and morally responsible fashion while representing the Company over the Internet.

### ***Software Licensing and Use***

Only software developed or licensed to Datamation and approved by Information Technology Management may be installed on Company computing resources.

# Company Information Security Policy

All employees are required to comply with software copyright laws and licensing agreements. **Unauthorized duplication of licensed software and documentation is strictly prohibited.**

All software developed by employees or contractors on behalf of Datamation is Company property and protected by copyright law from unauthorized use and duplication.

## *Virus Protection*

Company approved virus protection software must be installed, enabled and updated at least monthly to protect all Company computing assets from virus infection.

## *Access Controls*

Access control procedures must be established to protect data, software, and computing resources from loss, disclosure or misuse. Access to Company information and systems will be granted on a need-to-know basis based on job responsibilities.

## *System and Application Controls*

Change control processes must be used to minimize the risk of change and its impact on production applications and computer systems. Changes must be authorized, tested, and documented prior to implementation.

## *PC Laptop Security*

Company owned computers systems, including laptops and desktops, must be secured at all times to prevent loss of the computer and the sensitive information contained within.

## *Physical and Environmental Controls*

The environment surrounding all computing equipment, including mainframe, mid-range, servers, communication hubs, telecommunications equipment, etc., must be protected from accidental or intentional loss, damage or disclosure. Physical access to the room containing computer equipment must be restricted to authorized individuals. Environmental controls such as fire suppression, temperature and humidity controls, UPS, etc. must exist to ensure the minimal levels of downtime.

## *Telecommunications*

Datamation's telecommunication networks must be protected from any action that could jeopardize the integrity or security of company information.

Datamation is committed to protecting company assets and managing communications expenses. It is the ultimate responsibility of each company location to implement appropriate control over telephone service and related expense.

## *Information*

Company information must be classified based on its sensitivity and value to the organization (i.e., the business impact if destroyed,



# Company Information Security Policy

## *Identification and Classification*

damaged or disclosed). Classification of information will be used to develop appropriate levels of access control. The current classifications of information and applications are as follows:

- **Private** – applies to information about employees, customers, suppliers or the company that could adversely affect the company, stockholders, business partners, and/or customers.
- **Critical** – applies to information where incorrect information or disruption in processing could result in significant monetary loss, embarrassment to the company, criminal or civil liability, significant productivity loss, or impairment of operations. Information provided by clients in-order to carry out certain activities on behalf of the client.
- **Financial** – applies to information which processes and records financial information such as company assets, liabilities, equities, operating results, pricing, budget, forecast, etc.

## *Personal Data Protection*

All personal data of employees, customers, etc. must be obtained, processed, and protected in accordance with the standards outlined in this policy. In addition, employees must comply with any current or future privacy laws found in their resident countries.

All data systems remain the property of Datamation. There is no personal right of privacy maintained for any electronic equipment assigned to employees or the data stored on or created by that equipment. Datamation reserves the right to access and review any data retained or transmitted by its systems without prior notice, and disclose any information obtained to appropriate parties.

## *Segregation of Duties*

Segregation of duties must be maintained between incompatible functions in order to minimize the potential for errors and fraud.

## *Incident Handling*

Users should report any unusual computer or network activity to the Information Security Department as well as the Security Department. The Information Security Department, along with other technical staff, will determine if an actual event has occurred, conduct an investigation at the request of Human Resources or Security, make appropriate notifications and mitigate the risk of the incident.

## *Third Party Information Requests*

If Datamation information resources are placed in the custody of an outside entity, management will notify the outside entity of Policy and applicable Standards. Contracts shall specify the level of protection that the outside entity must provide for Datamation information resources while in the custody of the outside entity. Non-disclosure agreements and/or other applicable contracts must be established prior to providing access to company information.

# Company Information Security Policy

## ***Remote Access***

Remote access to all Datamation networks and resources may be permitted providing authorized users are authenticated, privileges are restricted, and data is encrypted across any public network (e.g., the Internet). This access must be approved in advance by the associate's manager or information owner. Such remote access is not a universal fringe benefit and may be revoked at any time for cause including unsatisfactory performance and non-compliance with security policies.

## **EXCEPTIONS**

Requests for an exception to this Policy or its Standards must be submitted in writing to the Information Security Department. These requests must include the reasons for the exception or variance and planned alternative control measures. Requests for exceptions will be handled on a case-by-case basis.

## **RELATED POLICIES**

Policies regarding information confidentiality and employee ethics are addressed in the Human Resource Policies Manual, Code of Ethics, and Integrity Handbook.

## **STANDARDS**

Datamation Standards shall be developed, reviewed, and revised, as necessary, to provide guidance for the implementation of Policy and to ensure compliance with the Policy.

## **REVISIONS**

The Policy and Standards will be revised as needed to reflect changes in the Information Technology environment and related business risks.

Changes to the Policy and Standards require approval of Information Security and Senior Information Technology Management.

Suggestions for revisions to the Policy and Standards should be forwarded to the Information Security Management.

## **DISTRIBUTION OF THIS MANUAL**

Information Security Management is responsible for publishing and distributing the Policies and supporting Standards.

The manual will be distributed electronically to all deptt

# Company Information Security Policy

heads within the HO and to the location managers in all-regional offices and franchisees.

A condensed version of the manual entitled “Company Information Security Policy Handbook” will be distributed to all employees of Datamation. This handbook summarizes various portions of the Information Security Policy and Standards and helps employees understand their role in protecting information.

## INTRODUCTION

User IDs and passwords are a critical part of ensuring the confidentiality, integrity, and availability of information resources. The Policy and Standards are intended to ensure that users recognize they are responsible for protecting their user IDs, passwords and other access codes entrusted to them. Users should select effective passwords to prevent guessing of the password by an unauthorized user. If an unauthorized user obtains an authorized user ID and password, actions such as deletion or modification of data could be performed under that user ID and accountability would be difficult to determine.

## POLICY STATEMENT

Each user must have a unique user identification code and password to access Company computer systems. In addition, users are responsible and accountable for all actions performed under their user ID.

## STANDARDS

### *User Accountability*

Each user must be issued a unique user ID and password to ensure individual accountability.

User IDs and passwords must be kept confidential.

Sharing user IDs and passwords is prohibited except in extreme circumstances and only with written authorization from management.

User IDs and passwords must not be posted or recorded where they can be viewed or accessed by others.

Passwords must be changed immediately when reset by a security administrator, or if it is suspected that the password has been compromised (i.e., observed by a third party).

Users must log off or lock their session whenever their computer is left unattended, i.e. use screen-saver passwords. See Chapter 6 for more information.

Users **must** turn off PCs or log off of all network resources at the end of **each** day.

Passwords should be constructed so that they are not easy to guess, but avoid passwords that must be written down to be remembered.

Do not allow others to look over your shoulder as you type your password. This is called shoulder surfing and can easily reveal

your password.

## ***Effective Passwords***

The following techniques can be used to create passwords that are not easily guessed but are still easy to remember.

1. Mix upper and lowercase letters and numbers. For example:  
Gold24K, Go2Store and Cat7Dog
2. Make up acronyms. For example:  
NOTFSW (none of this fancy stuff works),  
APEPAB (all programmers eat Pizzas and Burgers)
3. Select a series of words with a common theme. For example:  
Candy bars: KITKAT and BABOOL  
Cars: SONATA and ACCENT
4. Use the phonetic spelling of a word(s). For example:  
LITEBULB, EZRIDR, and TELIFONE
5. Make up compound words. For example:  
AIRPLAIN, MALEMAN, and RAILRODE
6. Replace certain letters for numbers in a typical word. Such as replace O with 0, I with 1, B with 8, S with 5, L with 7, or E with 3. For example:  
M0T0R5, ENG1NE, 8EAR1NG, and P1ST0N
7. Use regular words but omit vowels or other common letters. For example:  
NTRNT, MNTNDW, DATMAT, XPLRNG, and SCRTPLC
8. Use the first letter of each word from a line in a book, song, or poem. For example:  
"The Adventures of Huckleberry Finn : Mark Twain" would produce "TaoHF:MT" or "Who ya gonna call? Ghost Busters!" would produce "Wyc?GB!"

## ***Ineffective Passwords***

Easily guessed passwords must not be utilized as they increase the risk of unauthorized access to company computing resources and applications. To strengthen passwords:

1. Do not use your name, initials, user ID, nicknames, family names, addresses, months, or seasons of the year.
2. Do not use predictable patterns like: ascending or descending digits (1-2-3-4, 4-3-2-1), same character (55555), simple alphanumeric sets (W-X-Y-Z), using the abbreviation of a month along with the year (JAN98, DEC99), or keyboard sequences (qwerty, qwased, asdfjkl).
3. Do not use words associated with the Company such as DATAMATION, CUSTOMER, MNYL, INDIA, or GURGAON.
4. Do not use the following words as passwords: GUEST, SECRET, or PASSWORD.
5. Do not use any of the above examples spelled backwards, or in all capital letters
6. Do not use words chosen from English or foreign dictionaries, spelling lists, or other word lists and abbreviations.
7. Do not use other easily obtainable information. This includes pet names, license plate numbers, telephone numbers, identification numbers, the user's brand of automobile, and so on. Someone who knows the user could easily guess these passwords.
8. Do not use a password of all numbers, or a password composed entirely of alphabet characters. Mix numbers and letters.

## ***Managing Multiple Passwords***

There are many computer systems in use at Datamation. Each of these systems usually has its own security software that results in users having to remember multiple passwords. In order to use the same password on every computer system, it must satisfy the security restrictions of each computer used.

The security software on the mainframe has features that prevent users from selecting inappropriate passwords such as those mentioned above. Users selecting passwords that comply with the criteria documented in this chapter should meet the password requirements of all computer systems in use at Datamation.

## **RESPONSIBILITIES**

All users are responsible for complying with the Policy and Standards by:

- Following effective password management practices

- Keeping their user IDs and passwords confidential
- Familiarizing themselves with password standards described in the Access Control chapter of this manual

## REFERENCE(S)

See Chapter 6 Access Controls for more information on password security standards.

See Appendix : Laptop Security for more information on securing PCs and laptops.

## INTRODUCTION

The electronic mail (e-mail) systems provided by or used at Datamation are intended to assist employees and vendors in carrying out Company business by facilitating communication between individuals and work groups. The intent of this Policy and its Standards is to address the use of, access to, review, and disclosure of e-mail messages transmitted through Datamation's systems.

## POLICY STATEMENT

Corporate e-mail systems are to be used for Datamation related business purposes only. Datamation treats all e-mail messages sent, received, and/or stored in its systems as Company records. Corporate e-mail systems **must not** be used to continue, distribute or circulate **chain letters** and **inappropriate/offensive content**.

Datamation does not assure any personal right of privacy for any e-mail message or document transmitted through the use of Company equipment or systems. Datamation reserves the right to access all e-mail messages transmitted through Company equipment or systems, without prior notice, and to disclose the message to any person or entity that Datamation deems appropriate. Datamation retains the right to determine the acceptable use of its e-mail systems.

## STANDARDS

### *Management's Right to Access Information*

E-mail messages are Company records. The content of e-mail, properly obtained for legitimate business purposes, may be disclosed within the Company without user permission. Therefore, it should not be assumed that messages are confidential. Backup copies of e-mail messages may be maintained and referenced for business and legal reasons.

The Company may inspect the contents of electronic messages:

- In the course of an investigation triggered by the indication of impropriety, as necessary to locate substantive information that is not readily available by some other means
- In the process of correcting a problem with a respective electronic mail tool where no other alternative is available
- At any time the Company deems it necessary

Requests to access the content of electronic mail messages must be approved in advance by the Information Security Department or the Director of Human Resources.

### *Message Content*

The use of e-mail to transmit any message or file whose content violates any Datamation Policy or state or law is prohibited.



Examples of prohibited use include, but are not limited to:

- Communications that contain defamatory, sexually-oriented, obscene, offensive, threatening, or harassing language, pictures and/or videos
- Files that contain copyrighted materials for which required permission to use or distribute was not obtained

## *Message Integrity and Disclosure*

Incidental use of the e-mail systems to transmit messages of a personal nature will be treated by Datamation no differently than Datamation related business e-mail messages.

## *Safeguards of E-mail Systems*

Employees are prohibited from the **unauthorized use** of the password and encryption keys of other employees to gain access to other employee's e-mail messages. Only senior management can authorize such use.

Message encryption features of the e-mail system should be enabled when allowed by law.

Local copies of a user's database should be encrypted with medium encryption. This will prevent somebody from opening the local database without knowledge of the user's Notes password. The local database contains a replicated copy of the user's Notes mailbox and calendar.

## *Internet E-Mail*

The Datamation mail system can send and receive Internet mail messages. Unauthorized use of external mail services (examples: gmail, yahoo mail, etc) for company correspondence is expressly forbidden (authorization must be obtained from Information Security Deptt). To use Internet electronic mail appropriately, the following must be done:

- Treat all information put into Internet electronic mail as if it were publicly available information. Internet electronic mail is susceptible to interception, redirection, or loss. As a result, electronic mail through the Internet must **not** be used as a secure method of communications for sensitive information.
- Treat all electronic mail correspondence as if it is a potential record that can be used in litigation. (Legal precedents exist where electronic mail has been subject to discovery in lawsuits.) Do not put information in Internet electronic mail correspondence that you would not put on Datamation letterhead paper correspondence.

E-mail must **NOT** be used on the Internet to:

- Develop business processes that depend on guaranteed or reliable message delivery through the Internet unless the inherent unreliability of the Internet is accounted for in the process. Internet electronic mail is frequently delayed or lost and can **not** be counted on as a totally reliable message delivery system
- Send or receive information with inappropriate humor or graphics. Use of electronic mail on the Internet must be in accordance with other Datamation policies
- Distribute chain letters
- Distribute personal opinions that do not reflect the stated position of Datamation
- Distribute information that may be sensitive to Datamation

## *Other E-mail Considerations*

E-mail and electronic scheduling are excellent tools for communicating, sharing documents, and scheduling meetings. These tools can reduce the time required to share information and enhance business processes. However, information transmitted via e-mail can be vulnerable to a variety of security and confidentiality threats. Additional considerations when using e-mail include:

- Erasing a message from personal files does not necessarily erase all copies of the message. The message may have been forwarded, printed, or archived and may be stored for substantial periods of time
- Law does not establish a general right to privacy in the work place
- E-mail can be connected by gateways to other e-mail systems
- E-mail may include attachments in electronic form and may be saved as files in a directory that is not encrypted
- Computer viruses can be spread via e-mail systems
- E-mail messages can be "blind copied" to other e-mail users (E-mail can be forwarded without all recipients names displayed on the message).

## **RESPONSIBILITIES**

Local Area Network (LAN) and e-mail administrators are responsible for:

- Implementing safeguards that ensure proper use of e-mail systems and the protection of Company information

Department managers are responsible for:

- Ensuring that all employees and service providers comply with this Policy and its related Standards
- Notifying the LAN/e-mail administrator of terminated and transferred employees

User responsibilities are to:

- Comply with all company policies and standards
- Exit or password-protect their workstation when it is left unattended
- Delete e-mail messages within a reasonable period of time. E-mail messages, attachments, and calendars utilize disk space that is shared among many other users and must be treated as a shared resource
- Use e-mail consistent with its intended purpose. Do not use e-mail as a replacement for file transfer utilities. Attachments should be a business document of a reasonable size, not data files
- Change passwords in accordance with Company standards
- Use e-mail consistent with its intended purpose. Do not use an e-mail account assigned to another individual to either send or receive messages. Use features/facilities such as message forwarding to allow others read access to personal mail messages

## REFERENCE(S)

See Chapter 6 Access Controls for more information on password security standards.

See Chapter 3 for additional standards related to the e-mail over the Internet.

## INTRODUCTION

The Internet provides a vast store of information and can be used to conduct business as well as research services, customers, competitors, legal concerns and other business issues. However the authenticity and accuracy of this information should always remain suspect until verified through a reliable source. Due to the breadth of information stored on the Internet, precious employee time can be lost pursuing non-business issues or entertainment distractions. This standard is intended to address the appropriate use of the Internet for Company business purposes.

This Policy and Standards cover all Internet services. Examples of these services include but are not limited to electronic mail (e-mail), World Wide Web (WWW) browsing, transferring files via FTP, participation in news groups, Telnet, etc. Electronic mail via

the Internet is covered in primarily in Chapter 2 - Electronic Mail.

Authorized Internet users will behave in an ethical, legal and morally responsible fashion while representing the company over the Internet.

## POLICY

## STATEMENT

## STANDARDS

### *Acceptable Use*

Use of the Internet is for the support and improvement of Datamation business objectives. Access is a privilege, not a right and individuals are responsible for their behavior and actions when accessing and using the Internet.

To make acceptable use of these services, personnel must:

- Accept and support the policy that all files (data, software, etc.) downloaded from the Internet must be properly licensed to the Company and are considered a Company asset that is not transferable for individual use
- Refrain from accessing web and FTP sites that are not business related.
- Limit large multi-megabyte downloads to off-hours to conserve shared resources
- Comply with any copyright and software licensing laws.
- Utilize approved virus-checking software resident while connected to the Internet
- Protect sensitive Company information by using authorized encryption and authentication measures where appropriate under the guidelines developed by the Information Security Department
- Treat any information taken from the Internet as suspect until confirmed by a separate and reliable information source. This includes electronic mail messages and news groups

While using Datamation Internet services, personnel must

**NOT:**

- Use Internet services for illegal purposes. If someone is unsure of the legality of you're their actions, contact the Company Legal Department or Information Security
- Use another person's name, password, security keys, files, data or otherwise misrepresent your identity to other users or companies
- Use computer programs or devices to circumvent, subvert or disable any security measures anywhere on the network
- Intentionally engage in any activity that might be harmful to the computer or network systems or any of the information stored thereon. This includes, but is not limited to, creating or propagating viruses or worms, disruption or denial of services by intentionally overloading critical network systems or damaging files
- Use Datamation systems for commercial or political purposes not explicitly authorized by the appropriate Company management
- Download any previously unlicensed software package for evaluation or business use. All software must be evaluated and approved via an Information Technology project
- Use Company accounts or equipment to download entertainment software or games or play games over the Internet
- Upload and/or download graphics, images or other material that is inappropriate or not in accordance with Company policies
- Sell or distribute software through the Internet for personal commercial purposes
- Post or upload sensitive Datamation information to any public Internet service where it can possibly be intercepted
- Reveal the personal addresses or telephone numbers of employees or colleagues
- Store, post, display, transmit, intentionally receive or exchange pirated software, stolen passwords, stolen credit card numbers, indecent or obscene material or other information inconsistent with Datamation business

Authorized Internet users may participate in news groups or bulletin board services to exchange technical information and tips regarding products the Company uses (refer to the topic regarding Public Representation below). As a participant in these services you may offer non-proprietary and/or non-confidential suggestions regarding product usage. Whenever you post information to these

services, you must include the following statement:

**The information provided above does not necessarily represent Datamation Company nor does Datamation Company or the author support it. ANY USE OF THE PRECEDING INFORMATION IS AT YOUR OWN RISK. Use of this information may infringe on copyright or trademark rights; it is your responsibility to ensure your use does not infringe on someone else's rights .**

## *Public Representation*

Authorized Internet users who are expressly authorized by Company management to provide official support of our products or services may indicate their affiliation with Datamation in electronic mail messages as long as those offerings comply with the Acceptable Use provisions in Chapter 2. This may be done by explicitly adding certain words, or it may be inferred (for instance via an electronic mail message address). Datamation retains the copyright to any material created or electronically distributed by any authorized Internet user in the course of their duties. To avoid libel, distribution or transmission of negative comments or similar attacks on any person or entity, including Datamation competitors, is strictly prohibited.

Authorized Internet users must never publicly disclose sensitive internal Datamation information, whether via the electronic mail or other network service, including any information that may adversely affect Datamation's competitive position, customer/vendor relations or public image. Such information includes, but is not limited to, business prospects, product performance, product release dates and other similar information.

## *Infrastructure Monitoring*

All use of the Internet services, including electronic mail, is subject to observation and monitoring by Company Information Technology, Information Security and/or Internal Audit to verify that the use of services is in accordance with Company policy. The Company reserves the right to collect, monitor, examine, copy, store, transmit, print, and use any and all information entering, leaving, residing in, or processed by any and all information systems and components used in the Company setting for the purposes it determines appropriate, and at its sole discretion. **There is no privacy or expectation of privacy in the use of any Company information systems or technologies.**

The infrastructure supporting Internet access across the Company will be periodically reviewed and evaluated for effectiveness. Information Technology, Information Security and/or Internal Audit reserve the right to conduct audits of the internet services at

a frequency of its choice.

Should it become apparent that a security breach has taken place or is imminent, the following actions will/may take place:

- If sensitive Datamation information has been lost, or unauthorized use of Company systems has taken place, you must notify the local site/branch manager or the accounting manager immediately. Local management must forward a copy of the report to Information Security immediately.
- Internet access may be immediately terminated Company wide at the discretion of Information Technology management until the extent of the breach can be assessed.
- Internet access privileges may be revoked for individual users at the discretion of Information Technology and Information Security if it is deemed network security is being compromised through that user's account or files.
- Internet access privileges for any person or computer system suspected to be involved in a security breach will be immediately suspended and investigated.
- For security breaches originating internally, Information Security, Security and Human Resources will be immediately notified for investigative and disciplinary purposes.

### ***Requesting Internet Access***

Users requesting Internet access must fill-out the Internet Policy Acknowledgment form (See Appendix for Form). The form must be signed by both the user seeking Internet authorization and a manager with authority. Signing this form indicates the user and the manager have read and understood all relevant policies and standards pertaining to the use of the Internet. The signed form must be forwarded to the Information Security Department for processing.

### ***Internet Gateway Locations***

Basic Internet access will be provided through approved Internet gateways. The objective of is to provide a secure computing environment by minimizing the exposure to unauthorized access to company data and systems via the Internet connections. The Company's direction is to minimize the number of Internet connections, constantly monitor all Internet connections for intruders, apply patches to systems within the Internet gateway within two business days of their release and to manage and control all Internet connections.

### ***Internet Gateway Requests***

To request an Internet gateway implementation, submit a project charter to Information Security in HO for approval.

Information Security Deptt must approve and manage all projects in this regard. Additionally, the gateway must be managed and monitored by Information Security.

Locations that are not on the Datamation Wide Area Network may set up dial-up accounts to a local Internet Service Provider (ISP) if approved by Information Security. While using this dial-up connection, the workstation must not be connected to the Local Area Network. At the end of each quarter, the location must send the Information Security the number of approved dial-ups for that location.

## **RESPONSIBILITIES**

All users are responsible for:

- Reporting any known or suspected violation of this Policy and/or standard to the local plant/site manager or accounting manager and cooperating in the investigation of alleged violations.
- Complying the standards and policy regarding Internet access contained herein.

Custodians are responsible for monitoring traffic and taking actions to secure Datamation's internal network from unwanted Internet traffic.

Managers are responsible for:

- Taking action on the alleged violation and forward copies of the report to Information Security and the Company Legal department within two business days.
- Notifying the applicable Administrators of terminated or transferred employees.

## **REFERENCE(S)**

See Chapter 2 for more standards related specifically to E-mail over the Internet.



## **INTRODUCTION**

The Company Information Security Policy and these Standards are intended to address the proprietary nature and use of software that is purchased, leased, licensed, or developed by Datamation.

The reproduction of copyrighted computer software without required authorization violates copyright laws. Unauthorized software reproduction is an offense, and exposes both individuals and the Company to criminal penalties including fines and imprisonment.

The term "software" as used in this Policy and Standards refers to all copyrighted computer programs, user manuals, training manuals, data, and related material, which have been purchased, leased, licensed, or developed by or for Datamation.

## **POLICY STATEMENT**

Only software developed or licensed by Datamation and approved by the location's Information Technology Management may be installed on Company computing resources.

All employees are required to comply with software copyright laws and licensing agreements. Unauthorized duplication of licensed software and documentation is strictly prohibited.

All software developed by employees or contractors on behalf of Datamation is Company property and protected by copyright law from unauthorized use and duplication.

## **STANDARDS**

### ***Software Use***

Purchase only approved standard hardware and software to ensure it is supportable. This will minimize technical support response time.

All employees should be trained on software products prior to using them.

### ***Software Licensing***

All software installed on Datamation computers must be properly licensed, such as with a Company site license, server-based license, individual workstation license, or negotiated contract.

A sufficient number of copies of software must be purchased to ensure that it is used within the terms of the relevant licensing agreement.

For the majority of commercially available software packages, a customer purchases a license to use the software rather than purchasing the software itself. In many cases the media on which the software is shipped and the software documentation (e.g., user manuals) are sold as items separate from the software license. Although there can be no definitive statement on what constitutes proof of license, the following are likely to be acceptable in most circumstances:

- A software license certificate issued by the software author.
- A contract schedule outlining authorized software usage signed by the software author or authorized supplier.
- A signed software license agreement.
- A purchase invoice from an authorized software supplier containing details of valid software version numbers.
- A formal statement of authorized use of software purchased centrally by Datamation Information Technology for use throughout the Company.
- In most cases, possession of the media (e.g., CD) on which the software was delivered is proof of authorization to use a single copy of the software.

While locations may have more than one of these documents related to a single license (e.g., certificate and purchase invoice), this does **not** allow the location to use this as authorization to use more than one copy of the software.

In some cases, usually for older software, ownership of the user manuals is sufficient proof of license. This approach is less common nowadays and should not be relied upon.

Much software is purchased at favorable prices by way of Version Upgrades or Competitive Upgrades from products supplied by other software houses. Often in these cases the supplier of the new software does not ask to receive the old licenses and, therefore, a location may have proof of licenses for both the old and new software. In these cases locations must **not** continue to use the old software once having installed the new software.

The reproduction of copyrighted software is prohibited unless authorized within the terms of the licensing agreement.

Demo software obtained on a trial basis must be removed after evaluation unless properly licensed.

Department specific software and files must be removed from microcomputers that are transferred to another department.

## *Appropriate Software*

Personally owned software shall not be installed on Datamation-owned computers or equipment unless a business justification is documented and approved by location IT management.

Games may not be stored or used on Datamation computers, except for those that are included with software licenses by Datamation.

Public domain software, freeware, or shareware is not to be downloaded to Datamation computers from external networks, bulletin boards, or other sources.

## *Software/License Monitoring*

On a quarterly basis, locations must perform a software self-audit to determine the software loaded onto the PC and network computers.

Datamation Information Technology has purchased sufficient copies of a software product to cover all locations. Maintain a current, accurate inventory of all license information, as described above, and make it available for internal or external audit inspections.

Locations must maintain accurate records of the licensed status of all their installed software and update the central Notes database on at least a quarterly basis. Locations must be able to provide evidence of compliance to Company IT and/or Internal Audit upon request.

The source code for critical business systems must be acquired from vendors.

## **RESPONSIBILITIES**

Location IT managers are responsible to:

- Pursue non-compliance actions against any individual within the department who refuses to comply with this Policy
- Approval of all new hardware and software purchases
- Provide necessary training to employees on software products
- Ensure compliance with software license agreements by verifying that:
  - All copies of software used at the location can be related to a software license
  - Software is not accessed by more individuals than the software license permits
- Remove software that is not in compliance with these Policies and Standards.

Users are required to report instances of illegal use of software or documentation copyright infringement to department management. Users must comply with the policy and standards outlined.

## INTRODUCTION

The threat of computer virus attacks has increased dramatically in the last few years. The Virus Policy and associated Standards describe virus prevention techniques directed at minimizing the risk of virus infections to Datamation's information and computing systems.

## POLICY STATEMENT

Company approved virus protection software must be installed, enabled and updated at least monthly to protect all Company computing assets from virus infection.

## STANDARDS

### *Symptoms and Indicators*

A number of things can happen when a virus has infected or attempts to infect a computer even before any damage has been done.

Symptoms of event that could be caused by viruses are as follows:

- Unexplained system “crashes”
- Programs that suddenly don't work properly
- Data files or programs mysteriously erased
- Disks become unreadable

Indicators:

- File size increases
- Change in “Last Updated” or “Modified” time and date stamp
- Sudden decrease of free space – when running a new program, particularly freeware or shareware, be alert for a sudden, unexpected decrease in free disk space or available memory
- Numerous unexpected disk accesses
- Strange macros attached to files

### *Prevention*

Anti-virus software shall be installed on all microcomputers (desktop and portable) and LAN servers connected to the WAN and stand-alone systems.

Anti-virus software pattern files must be kept current. The pattern files must be updated at least monthly. However, pattern files should be updated as they are available (i.e. weekly). These files require regular updating to protect against new viruses that appear regularly.

File servers and application servers must be set up to continuously scan executable files and scan all files prior to running backups. A full scan of servers should be scheduled on a weekly basis during non-peak hours.

Workstations must be configured so that files (hard drive and removable storage media) are automatically scanned by virus protection software before they are opened. If this is not possible due to hardware constraints, workstations must be scanned for viruses at system start-up and every time a diskette or CD is inserted.

All diskettes or CD's, regardless of where they come from, must be scanned for viruses before they are used. This includes demo software, shrink-wrapped software, diskettes/CD's used on home computers, as well as diskettes/CD's received from other Company departments.

Diskettes or CD's intended for mass distribution must be validated to be free from viruses prior to distribution.

Following the repair of a microcomputer, the equipment must be validated to be free from viruses before use.

Files should be periodically backed up. It may be necessary to restore the system from backups after a virus infection.

Users should be prevented from modifying executable files on LAN servers whenever possible. This prevents an infected User PC from infecting a file server.

Infected files must be either auto-cleaned or quarantined.

Only authorized IT personnel should be permitted to modify the virus protection software configuration.

New virus protection signatures should be tested prior to installing on production servers. However, in the event of a virus outbreak in may be necessary to forgo testing.

Updates must be pushed within 2 days of virus emergency and outbreak to mitigate the risk of information loss and disruption.

Auto Response should be setup, where possible, to notify appropriate IT personnel of virus events.

Do not read, open or forward emails suspected to contain a virus or from an unknown source. Contact the IT Help Desk for assistance if necessary.

Employees who use their home computer for work-related purposes must install virus software on their home computer,

especially if connecting to the company network remotely or bringing media home for work.

## **RESPONSIBILITIES**

Datamation currently has a McAfee anti-virus scanning software. Contact Company IT for this software.

IT Managers are responsible for complying with the Policy and these Standards by:

- Reporting all new virus infections to Information Security or the IT Help Desk
- Comply with Company licensing agreements
- Installing the anti-virus software and updates in accordance with these Standards and the licensing agreement(s)

Employees are responsible for complying with the Policy and these Standards by:

- Reporting all detected or suspected viruses to location IT managers
- Scanning all files and storage media for viruses before they are used

## INTRODUCTION

Access to computer records and equipment can be established through various methods. This includes physically restricting access to computing resources and restricting an individual's access to information after they enter a system. The intent of this policy is to protect company data from accidental or intentional loss or disclosure and to protect company computers from unauthorized access or physical damage.

## POLICY STATEMENT

Access control procedures must be established to protect data, software, and computing resources from loss, disclosure or misuse. Access to Company information and systems will be granted on a need-to-know basis based on job responsibilities.

## STANDARDS

### *Acknowledgment of Non-Disclosure Agreement*

All employees, vendors, customers and/or contractors assigned to Datamation assets should have on file either in the Legal Department or Human Resource department, a signed, legally binding information non-disclosure agreement. The signed agreement must be in place prior to any access privileges being granted.

### *Identification and Authentication of Users*

Automated access control systems that incorporate unique identification and authorization methods, such as a user ID and password combination, must be used for controlling access to computer systems.

Each User must be assigned a unique sign-on ID and password to ensure accountability.

Users must change their initial password to a new confidential password during their first use of a sign-on ID.

Computerized systems should allow users to change their own passwords.

The following minimum standards apply to passwords:

- Passwords must be at least 6 characters in length
- Passwords must be changed at least every 60 days
- Passwords must be stored in encrypted format
- Passwords must not be equal to user ID
- Passwords must not be displayed in clear text
- Passwords must not be printed on system reports

A complete set of access control and password standards for specific hardware/software is contained in the appendices.



Information Security Administrators should not have access to computer system user passwords.

A positive verification of the user is required for all password resets to ensure that the user is the actual owner of the user ID being reset.

Vendor-supplied default and system initiation passwords must be changed immediately after system installation.

Access control software should prevent consecutive re-use of passwords. Whenever possible, users should not be able to reuse a password within one year or 8 cycles of the changing of that password.

User IDs must be disabled or suspended after 5 unsuccessful access attempts.

One of the following features must be employed:

- Users must logout when leaving their PC unattended for any period of time
- If applicable, “Lock the Computer” when leaving the machine unattended. This feature is available within Windows NT/2000/XP
- After 10 minutes of inactivity, user PC screen-savers with passwords should be activated, or
- After 10 minutes of inactivity, Business application sessions should be locked until a user’s password is re-entered

After 30 minutes of inactivity, any business application session should automatically terminate.

User IDs will be suspended after 60 days of non-use and deleted after 180 days of non-use.

User IDs and passwords should not to be hard coded or embedded into software, login scripts, macros, batch files, or function keys.

Periodic reviews (at least annually) of access granted to users must be conducted.

Users will be prevented from logging on to an application from more than one workstation at a time, wherever possible.

Where available, users should be notified of the last time their user ID was used. Discrepancies found should be brought to the attention of their Information Security Administration department.

Access to computer resources including data must be canceled immediately upon notification of termination date, date of transfer to a new department/group at Datamation, long-term leave of absence, or layoff.

Contract employees (if any) should utilize an expiring ID. Upon the renewal of the contract, access capabilities should be extended to allow for uninterrupted access to computer resources.

IT employees and contractors should have an extensive background check performed prior to being hired or contracted with Datamation.

Access to computer resources must be kept current as employees change job assignments. Human Resources should notify Information Security and/or appropriate IT personnel of employee and/or contractor changes in responsibility or job termination.

Security systems must provide an audit trail of all:

- Unsuccessful access attempts
- Successful access attempts to critical resources
- Access violation messages
- User ID logons
- User ID logoffs

The logs should include who attempted the access and when.

Security violation logs must be reviewed by the security administrator at least weekly to ensure the system is not being compromised. The logs should be protected from unauthorized access and retained for at least 6 months.

Any procedure designed to bypass established identification and verification routines, such as automating the entry of an ID and password through a workstation, is prohibited.

## *Data and Software*

Access to production software libraries/directories must be restricted.

Adequate segregation of responsibilities must exist so that systems and programming personnel do not have update access to production data or software libraries/directories on a normal basis.

Production data will be updated only by a production job or through a controlled process.

Data storage media must be stored in a secure location when not in use.

## **RESPONSIBILITIES**

**Owners** are responsible for ensuring that custodians implement access control measures to protect information resources.

**Custodians** are responsible for implementing effective access security systems/controls that:

- Incorporate identification and authentication techniques
- Provide individual accountability
- Safeguard against repeated attempts to break passwords or access codes
- Notify Information Security of inappropriate access attempts or security violations
- Restrict access to information as determined by the information Owner
- Protect computing resources from environmental dangers

**Managers** are responsible for reporting employee terminations and transfers to system security administrators.

**Users** are responsible to:

- Never leave an active workstation logged on and unattended
- Manually enter their password when they log on (do not automate this process through the PC or workstation)
- Follow effective password management techniques

**REFERENCE(S)** See the appendices for information on configuring the security settings on various hardware/software platforms.

## INTRODUCTION

To ensure the integrity of production information, new system development or changes to current application systems must be implemented in a controlled fashion. Effective change management processes are those that increase the probability that systems will function as intended and reduce the risk that unauthorized changes to programs and data will occur. The change management process is designed to protect against losses, damages, or inaccuracies that can occur through error or fraud. The Policy and following Standards describe the minimum control requirements for managing changes to production computer systems.

## POLICY STATEMENT

Change control processes must be used to minimize the risk of change and its impact on production applications and computer systems. Changes must be authorized, properly tested, and documented prior to implementation.

## STANDARDS

### *Segregation of Duties and Key Dependencies*

System maintenance responsibilities and production change control activities should remain segregated so that the person performing the change does not implement the change into production.

System maintenance responsibilities and financial operations functions should remain segregated so that personnel performing system maintenance do not have responsibility for other operational functions (e.g., posting/approving general ledger entries, updating production data).

Each key system support person should have a trained backup for ensuring adequate system support and minimizing key dependencies.

### *Change Control*

All major system modifications and new development efforts must be approved by senior management. In addition, project charters, work plans and monitoring procedures must be implemented.

Master source program code and executable program code (object or load modules) must be kept in separate libraries that are protected by software that controls code modification.

All system and program changes must be supported by a written request from the data owner. An exception to this standard is modifications made to meet new hardware or software requirements or system enhancements. Although this maintenance does not require a written request, management must approve it,

and the owner and users notified of the change.

All changes must be made using a secondary copy of the production source code, not master source or executable code.

Testing must only be performed using test data and test versions of programs. For reporting or “read-only” programs, it may be practical to test changes using production data.

A control register must be maintained that identifies:

- The application affected
- The reason for the change
- The person authorizing the change
- The person making the change
- The person reviewing/approving the change
- The date the change was effective

Multiple program change requests can be pooled under one control number. Documentation of the change indicating the programs involved and a description of the code changed must support the control register. This documentation must be kept for at least one cycle such that all programs have documented support.

The production program update must be reviewed and authorized by someone other than the person who made the code changes.

System changes that affect the controls of the system must have test results reviewed and approved by users before the update is made to the production executable program code.

All users need to be informed of new changes scheduled into production.

There must be verification that the source and object libraries are updated properly. Audit trails of changes must be provided including date and time or version number.

In emergency situations the program changes applied must evidence the review and approval after the change was made. These provisions are designed to ensure that changes to production are adequate and appropriate.

Provisions must be made to “back out” program components so the prior production version can be restored or recreated.

### ***Internet Application***

Applications developed for internal (Intranet) or external (Internet)

## *Development*

use must adhere to the following guidelines:

- Applications must be designed and implemented with approved software defined by Company Information Technology
- Applications designed to convey information to a significant portion of the Company must:
  - Be approved by Company Communications for content appropriateness
  - Control access to restricted information based on user-name/passwords
- Applications that are essential to specific business functions or procedures, must be hosted on systems that are maintained and backed-up by Information Technology. However, if applications or functions are out-sourced, legal contracts must exist to ensure the protection and integrity of confidential Datamation information.
- Applications developed as Internet applications designed to be used from outside the Datamation Company network must adhere to these guidelines:
  - Applications must be approved by Company Information Technology
  - Applications accessing sensitive information must encrypt the information traversing the Internet between the endpoints of the target user and Datamation
  - All applications developed for the Internet must be approved by Company Communications for content appropriateness if the application speaks for the Company or as the Company.
  - Applications using encryption and authentication security must have sign-on warnings in the application that warns the user of the application that unauthorized use is prohibited.

## *Operating Systems and Application Patch Updates*

All operating systems should be running with the most current patch release to ensure that security holes are closed as soon as possible.

System Administrators or location IT management should obtain patches from the software vendor at first release. Testing of the patch should be implemented to prevent adverse reactions in the production environment.

## *Documentation Standards*

New application systems as well as applications under development must not be moved into production until there are adequate training materials and operating documentation. The minimum documentation standards are as follows:

- Application Operating Instructions – a list of specific job

tasks, run procedures, and schedules that are necessary for operating the application

- System Operating Instructions – a list of tasks and procedures that are necessary for operating the computer system
- User Manual – directions that describe how to process transactions and use the application
- Program Documentation – a description of the application program that indicates its purpose, scope, file relationships, and interface requirements
- Contingency Plan – instructions for restarting and recovering application processes following interruptions

## ***Internal Application Security***

Application software (whether purchased, leased, or developed by Datamation) must make use of the system access control facilities instead of the application's internal security.

## **RESPONSIBILITIES**

Owners are responsible for:

- Testing and approving system maintenance changes before implementation to production
- Assuring that the Custodian establishes an adequate change control process for managing system maintenance activities

Custodians are responsible for:

- Implementing and enforcing a change control process
- Protecting production libraries/directories through adequate access control restrictions
- Ensuring that adequate documentation has been established
- Segregating system maintenance responsibilities so that the person performing the change does not implement the change into production
- Adequately segregating the test and production environment

Departments that operate their own computer systems may have both Owner and Custodian responsibilities. Therefore, they are also responsible for segregating system maintenance responsibilities so that personnel performing system maintenance do not have responsibility for other operational functions (e.g., posting/approving general ledger entries, updating production data).



**REFERENCE(S)** See Chapter 6 – Access Control for more information on protecting data and software.

Chapter 12 for additional information on Segregation of Duties.

## INTRODUCTION

Computer processing facilities must be protected from unauthorized access and environmental hazards that might cause disruption of business processes. Access restrictions should be designed to physically restrict access to computing resources. The computer environment and related equipment must be protected from hazards such as fire, humidity, physical damage, etc.

## POLICY STATEMENT

The environment surrounding all computing equipment, including Main Server, mid-range, file servers, communication hubs, and telecommunications equipment must be protected from accidental or intentional loss, damage or disclosure. Physical access to such equipment must be restricted to authorized individuals. Environmental controls such as fire suppression, temperature and humidity controls, UPS, etc. must exist to ensure minimal levels of downtime.

## STANDARDS

For the purposes of these standards, controls required over computer processing centers are described in three categories.

### **Fire Protection:**

- Controls to be applied to the computer facility to mitigate the risk of fire

### **Access and Security Protection:**

- Controls to be applied to the computer facility to eliminate or reduce risk of unauthorized entry to the facility

### **General Environment Protection:**

- Controls to be applied to the overall computer facility, not specific to fire, security, or access

### **Computer Room Differentiation**

The controls surrounding computer equipment should vary based on the overall business risk and size of the computer room. For instance, major data centers must implement all controls within this policy and standard while smaller computer rooms or telecommunications closets at locations may only need to implement a limited number of physical and environmental controls. While determining the level of controls to implement within any computer room or telecommunications closet the business impact and risk should be assessed. While determining risk, the following factors should be taken into consideration:

- a) The criticality of the data and systems that are present at the site (e.g. could the plant operate for several days without the systems?)
- b) Whether the financial and manufacturing applications are contained on resident systems?
- c) Whether the facility supports other locations?
- d) How heavily the plant depends on its resident systems for 'just in time' manufacturing operations?
- e) Impact to suppliers, customers, and other plants if the

information contained on the resident systems are unable to be retrieved?

- f) Other geographical threats such as earthquake, volcano, tornado, flooding, etc.

Locations should consult within Information Security and Company Information Technology management if necessary in order to determine appropriate physical and environmental controls.

## ***Fire Protection***

- Smoking is prohibited inside the office premise.
- All doors, partitions, floors and other construction are to be non-combustible (preferably)
- Adequate number of fire extinguishers to be installed at key locations.
- Fire extinguishing systems should be checked and certified annually.
- At least one fire extinguisher of the Carbon Dioxide type should be available within at least 50 feet of any point in the computer room.
- Annual inspections by the fire department.
- Highly flammable materials such as paper or cardboard should not be stored in the computer room.
- The computer room must be restricted at all times to only those who need access to perform their job function.
- Data files, programs, disks, documentation, etc. critical to the continued operation of the data center must be identified and protected by remote storage.

## ***Access and Security Protection***

- Entry to the office premises will be restricted by putting Security Guard at the main gate.
- Visitors to be given an entry into the office after taking approval from the person concerned.
- Visitor details to be logged into a register at the security gate.
- A visitor's badge to be provided to each visitor
- Bags and other belongings of visitors and employees have to be thoroughly checked by the security guards while entering and leaving the office premises.
- Sensitive reports and data must be protected from unauthorized access (i.e., not stored in unprotected locations.)
- Server system (boot) disks should be safeguarded and separate from the server to prevent users from rebooting the system and bypassing the server console logical security controls.
- Pre-employment investigations should be conducted for employees hired to perform computer system support work. Checks should include previous employment record, educational background, and criminal record.
- Visibility into the computer room must be eliminated.
- Windows located on outside walls must be sealed with brick or other attack resistant material.

## ***General Environment Protection***

Through the use of environmental controls, security and protection of the computer room and the equipment within it will be greatly increased.

Environmental control guidelines are as follows:

- Temperature and humidity should be controlled according to the equipment manufacturer specifications
- Temperature and humidity controls should be tested periodically or certified by the vendor
- Perimeter barriers (walls) must extend from the floor to the constructed roof above (not the dropped ceiling)
- Emergency procedures must be developed and posted in an appropriate visible location, detailing specific action to be taken by employees in the event of an emergency
- An uninterruptable power supply (UPS) or alternate power source should be used to protect against loss of critical services because of power outages. For extremely critical systems, the availability of a generator backup may be desirable
- The UPS system or generator should be tested periodically (at least once per year)
- Packages delivered to the computer facility are not to be opened directly in the computer room
- Surge suppressers or voltage regulators should be used on critical hardware components to protect against power fluctuations
- Emergency lighting should be provided

- A power disconnect button properly labeled should be located at the principle exit doors and should also be covered or protected to ensure the power is not accidentally shut off

## **RESPONSIBILITIES**

The Owner has the authority and responsibility to:

- Specify control requirements based on classification and criticality of the systems processing their information, and communicate these requirements to the information Custodians
- Assure that Custodians provide reasonable security measures to protect information resources

Custodian responsibilities are to:

- Establish adequate security controls to protect the information resources for which they have custody
- Manage and protect information assets on behalf of the information Owner

## INTRODUCTION

Business communication is a substantial expense to Datamation each year, and failure to control these costs can effect the profits of the Company.

With the continuing increase in telephone fraud and misuse of company communication assets, there is need to manage telephone use and costs throughout the company. Telecommunication monitoring involves security over the telephone system, review of service provided by the carrier, and review of the costs associated with providing telephone service.

## POLICY STATEMENT

Datamation's telecommunication networks must be protected from any action that could jeopardize the integrity or security of company information.

Datamation is committed to protecting company assets and managing communications expenses. It is the ultimate responsibility of each company location to implement appropriate control over telephone service and related expense.

## STANDARDS

### *Voice Communications*

The objective of this policy is to:

- Provide guidelines for telephone system administrators to define the use of the telephone system at the facility.
- Provide guidelines for employees in the use of company telephones and communications assets, and
- Establish guidelines to monitor the expenses associated with the telephone system.

### *Telephone Maintenance*

Each location should have the following essential information, regardless of whether the location depends on a third-party telephone maintenance company.

- Full set of technical manuals for PBX and Voice-mail / Auto Attendant systems which are in operation. These are needed to verify default settings.
- Contact information for customer services, technical assistance and accounting information, including account manager
- Copies of all maintenance contracts / purchasing agreements for all services provided
- Diagram of system and inventory of all equipment under the care of third-party provider

- Current version / release level of all telecom-related software
- Number of trunks in the PBX and the extensions attached to them
- copies of trunk routing tables and Class of Service definitions by extension
- PBX trunk traffic reports (where available)
- Remote access port information (port, trunk, number), and information relating to the changing of remote access password, as well as security settings
- Instructions on how to obtain detailed usage reports by extension. If this is not a feature on the current system, management should consider finding an alternative method of gaining this valuable information. (It is NOT sufficient to rely on the service provider's periodic bill for detailed information on telephone usage or costing – usage bills arrive too late and do not allow us access to view information instantly, in the event of a security breach.) Bills should be compared to internal reports, to allow us to verification of their accuracy

The telecommunications manager or person responsible for the telephone systems must receive adequate training and has sufficient skills to perform the job function. An alternate person must be able to act as support in the event of an unscheduled absence of the main telecommunications manager.

Preventative maintenance must be performed annually on all telephone equipment (PBX and Voicemail system).

For large PBX systems, the telecommunications manager must periodically review the PBX traffic reports and evaluate appropriate utilization in the efforts to minimize cost and impact to the business. He/she should verify whether there are:

- trunks with low peg counts or little or no traffic
- times when all trunks are busy
- times when the dial tone delay is more than ½ second
- excessive service queue lengths
- examples of calls being abandoned to the operator

### ***Voicemail Access***

The voicemail system controls should include the following:

- Requires passcodes to be at least 4 characters long

- Prevents passcodes from being easily guessed e.g. repeating characters, same digits, and the same as the extension
- Voicemail passcodes are never “spoken” by the system (no audio response of the passcodes)
- Disables the voicemail box after a predefined number of unsuccessful access attempts occur
- Administrative passcodes have been changed since the last vendor maintenance date
- Passcodes are encrypted when stored and during transmission
- Does not have default passcodes still enabled

The Voicemail system should be configured such that a person accessing a voicemail box cannot bridge over to the PBX to obtain a dial tone and outside line.

### ***PBX Access***

The PBX should be configured to allow calling features and long-distance access to only those who required such access to perform their job function. Classification will include:

- International calls
- Long Distance numbers
- Local numbers
- Mobile number
- Only Internal numbers



Remote Access Ports, which are generally used for maintenance, should be secured. The following are controls that should be implemented on these ports.

- default system passwords have been changed
- passwords are changed immediately after vendors perform maintenance
- the phone number for the access port is secured (i.e. not written down on the modem, posted on bulletin board, or posted on PBX door)
- passwords meet with required standards
- passwords are encrypted when stored and during transmission
- passwords are never “spoken” by the system (no audio response of the passwords)
- system disconnects you after predefined number of unsuccessful attempts
- system changes via the port must be monitored by staff
- maintenance logs or audit trails must be kept for each external access point, to allow for full authorization and accountability of system access
- remote access port(s) is/are disabled when vendor/carriers are not performing maintenance

It is the location’s responsibility (NOT the third-party provider’s) to ensure that passwords are changed each time access is granted and revoked.

All system administrative default passwords must be changed since installation. Consult manufacturer’s manuals for more information on this subject.

A telephone usage policy should be developed and communicated to all employees including the attendant / switchboard operator to

## *Telephone Cost Management*

A telephone usage policy should be developed and communicated to all employees including the attendant / switchboard operator to ensure that they are aware of the following rules:

Employees should not be allowed to:

- Accept collect calls (unless in the case of an emergency)
- Accept third party billing (example: Party 1 calls Party 2 but Datamation is billed for the charge)
- Use company calling cards for personal calls

The billing telephone company or the third-party PBX system company should supply the location with the following monthly information to provide proactive monitoring of telephone charges with the objective of identifying telephone abuses, possible break-ins, and cost savings.

You may need to contact the service provider and discuss availability of these reports:

- telephone extension usage after-business hours
- telephone extensions with little or no activity
- telephone extensions with high call volume
- telephone extensions with long call duration
- third party billing (1800 numbers)
- international and long-distance calls
- suspicious calls or unknown area codes

The telecommunications manager should periodically verify the accuracy of the external phone charges by comparing phone bills with the data from the internal PBX / Auto-attendant Cost Detail Reports.

Phones located in unoccupied or semi-public areas of the organization should be restricted from making international, long distance, operator-assisted, and in many cases, even local toll calls.

## *Telecommunications User Management*

The Local Human Resource employee termination process should account for the following telecom resources:

- telephone extensions
- mailbox accounts
- authcodes
- calling cards
- cellular phones
- pagers

Access to these resources should be returned, disabled or deleted promptly upon the user's termination.

The telecommunication manager should review access to these resources on a regular basis.

## *US Long Distance Telephone Charges*

For US locations, all long distance charges should be billed at the rates negotiated by Datamation .

- All US locations should be using the Company long distance plan rates.
- If the Datamation plan is being used, the complete volume of Datamation telecommunications will be considered in the contract negotiations.
- The bill will be sent to the location for verification of the expense and approval prior to Accounts Payable processing.
- The bill should include detail of phone charges to be used for identifying telephone abuses, possible break-ins, and possible cost savings. If detail is not included, contact Sushma (011-43038800).
- If the FM Company plan is not used, then your location may be paying a higher rate plus your location volume is not considered in the negotiations for new rates.
- Any long distance charges on a local telephone carrier's (MTNL, AirTel etc) invoice is billed at the retail rate. Contact Sushma to get the phone numbers added to the DM Company plan.

## *Problem Resolution / Disaster Recovery*

The following should be included in the department procedures manual and the disaster recovery plan:

- An up-to-date vendor contact list to assist in problem resolution
- Problem reporting and escalation activities including procedures to address problems that occur outside normal business hours
- Backup and restoration procedures for the PBX and voicemail / auto-attendant software including for a full software re-load

The telecommunications manager should have a file documenting all service orders and system interruptions. The telecommunications manager should track these to identify hardware subject to repeat failures.

Equipment should be backed up on a periodic basis and backups should be stored off-site in a safe, secure location.

## **RESPONSIBILITIES**

IT managers are responsible for ensuring adequate authentication and accountability controls are in place for system users who must connect to the Datamation internal network.

Custodians, managers and users are responsible for complying with the Policies and Standards.

Telephone System Administrators must:

- Have a full understanding of the telephone system. They must be familiar with all the options available from the carrier such as use restrictions, its options, its settings and the expenses associated with providing telephone service to the facility
- Publish rules and guidelines for telephone use by employees

Management must:

- Understand and support the need for telephone system controls and recognize that cost control is a necessary part of Datamation's overall business objectives
- Regularly (at least quarterly) review the billing analysis available from the service provider for improper traffic patterns and improper use

The Telecommunications department must conduct an annual review of telephone service and options available from the service provider in the United States. For other countries, local sites must review service and options annually with in-country telephone companies.

## REFERENCE(S)

See Appendices for standards specific to certain platforms.

**INTRODUCTION** It is essential that adequate controls be provided to safeguard the integrity of data being processed through company computers. The possibility of direct financial loss, faulty management decisions or embarrassment to the company from disclosure of information must be minimized through the use of sound data protection methods.

Classifying information is the process of matching the assessed significance of the data to a level of access controls needed to protect it. It is the responsibility of the owner of an application to assess that need on behalf of the Company.

## **POLICY STATEMENT**

Company information must be classified based on its sensitivity and value to the organization (i.e., the business impact if destroyed, damaged or disclosed). Classification of information will be used to develop appropriate levels of access control. The current classifications of information and applications are as follows:

- **Private** – applies to information about employees, customers, suppliers or the company that could adversely affect the company, clients, stockholders, business partners, and/or customers.
- **Critical** – applies to information where incorrect information or disruption in processing could result in significant monetary loss, embarrassment to the company, criminal or civil liability, significant productivity loss, or impairment of operations.
- **Financial** – applies to information which processes and records financial information such as company assets, liabilities, equities, operating results, pricing, budget, forecast, etc.

## **STANDARDS**

All information must be classified, by its owner, as either sensitive or non-sensitive information. Sensitive information defined below as critical, financial, or private, must be protected from disclosure, modification, or destruction. Non-sensitive information or applications should conform to sound business practices.

### ***Sensitive Applications or Data***

**Private** - This classification is to be applied to applications or data about employees, customers, suppliers, or the company where loss, unauthorized modification, or disclosure to unauthorized parties could adversely affect the Company, its stockholders, its business partners, and/or its customers and cause loss or embarrassment to the Company. The use of this data must be in compliance with relevant statutory/regulatory requirements within the local area.

Examples:

- Customer financial or account information, strategic operating and marketing plans or personnel records (salary, medical, etc.)

**Critical** - This classification is to be assigned to information where incorrect information or disruption in processing of the application could result in substantial expense, embarrassment to the company, a violation of any agreement with Clients, or impairment of operations.

Examples:

- Production scheduling, Database, Original data provided by clients, warehouse management.

**Financial** - This classification is to be assigned to information which processes and records financial information that must be protected against unauthorized modification or disclosure, or produces statements of the companies assets, liabilities, equities, operating results, or provides pricing, budget, or financial forecast information.

Examples:

- Pricing, product costing, accounts payable, accounting information, profit forecasting, application accounting systems (General Ledger, etc.).

Information retains its classification regardless of the method of storage, transmission, or processing.

## ***Information Owner, Custodian, Users, and Managers***

All information must have an identifiable owner. The owner, in most instances, will be the business unit primarily accountable for the business results achieved when using this information. They are responsible for the definition, use, and integrity of the data.

The **Owner** is responsible for identifying, classifying, authorizing access to, authorizing custody of, and protecting information resources within the scope of their authority.

**Custodians** are individuals, generally IT personnel, charged with the processing, storage, communication, or presentation of information. Custodians must ensure that information assets are protected and managed on behalf of the information asset owner as to provide the information's accountability, accuracy, and integrity. For example, computer operations managers have safekeeping responsibility for information resources such as magnetic data, program code, and computing devices. Information Security Administrators can be viewed as custodians for security

administrative functions. The security administrators grant access to information resources based on the owner's authorization.

**Users** are individuals utilizing information or automated systems for an authorized business function. Users must comply with owner and custodian rules regarding information use.

**Managers** are individuals assigned the responsibility of managing system users. Managers are responsible for monitoring system users and ensuring compliance with the rules and guidelines regarding information use.

## *Controlling Access to Sensitive Computer Information*

Access to sensitive information and data files must be authorized by the owner of an application in accordance with its classification. This access approval must be documented in some verifiable form (e.g., signed memo, electronic mail).

Information should retain the same level of security even if it is copied or moved from one computing platform to another (e.g., down-loaded from the mainframe to a personal computer).

## *Information and the Internet*

Wiretapping and message interception are easily done and frequently encountered on the Internet. Accordingly, Datamation's sensitive information must not be sent over the Internet, via electronic mail or by other means. Credit card numbers, telephone calling card numbers, internal log-in passwords and other parameters that can be used to gain access to Datamation's network, stand-alone computers, accounts, goods or services must not be sent over the Internet in readable form.

Datamation software, documentation and all other types of internal information must not be sold or otherwise transferred to any non-Datamation party for any purposes other than business purposes expressly authorized by Company management. Sensitive information must not be transmitted to other Datamation employees who do not need to know this information. Authorized Internet users must exercise a greater degree of caution in this regard, given the reduced human effort required to redistribute such information electronically. Always use care in addressing electronic mail messages to ensure confidentiality is not accidentally breached.

## *Information Disposal*

Information must be disposed of in a manner that protects against its disclosure or misuse. When "Private" information is no longer needed but is still sensitive, the method used must assure that the

data is destroyed beyond recognition and cannot be reconstructed.

Information stored on electronic media (tapes, disks, etc.) is usually destroyed by "degaussing" or "overwriting." This method must be used for any electronic media that is reused to provide information to an outside entity. Additionally, the hard disks of all laptop and desktop PC's **must be overwritten** before they are reissued to another department, returned at end of lease, or disposed of. Simply formatting the hard drives is not sufficient. Inexpensive commercial software is available for this.

Note: Commands to delete or erase a file simply delete an entry in the file allocation table or catalog. Delete commands do not delete the actual data.

Information in hardcopy format (paper, microfilm, microfiche, etc.) must be shredded, incinerated, or disposed of in waste containers that the Company has designated for information destruction.

## RESPONSIBILITIES

The Owner has the authority and responsibility to:

- Judge the value of the information and classify it accordingly.
- Authorize all access to the information.
- Ensure that information system controls are designed into mission-critical software applications.
- Act as the official representative of this data in discussions pertaining to its interpretation or use.
- Specify control requirements based on classification and criticality, and communicate these requirements to the information Custodians and Users.
- Assure that Custodians provide reasonable security measures to protect information resources and that Users comply with procedures established for such protection.
- Negotiate performance and service level criteria with the Custodian.

Custodian responsibilities are to:

- Establish adequate security controls to protect the information resources for which they have custody.
- Implement access restrictions to information as authorized by the information Owner.
- Manage and protect information assets on behalf of the information Owner.
- Meet agreed upon reliability, performance, and availability requirements specified by the Owner.



User responsibilities are to:

- Use the data in a manner consistent with its intended purpose.
- Comply with controls established by Owners.
- Keep sensitive information confidential.
- Comply with information security policies, standards, and procedures established to protect the information resources being used.

All employees are responsible for information security and will be held accountable for the accuracy, integrity, availability, and confidentiality of the information to which they have access.

## INTRODUCTION

Personal data of employees and customers is collected, transferred, and stored throughout Datamation. In order to protect the privacy rights of those individuals and to reduce the risk of misuse of that information, proper care must be taken. This policy provides international guidelines for personal data protection. Data is considered “personal” if it is unique to an individual or company, such as name, address, telephone number, credit card number, birth date, etc.

## POLICY STATEMENT

All personal data of employees, customers, etc. must be obtained, processed, and protected in accordance with the standards outlined in this policy. In addition, employees must comply with any current or future privacy laws found in their resident countries.

All data systems remain the property of Datamation. There is no personal right of privacy maintained for any electronic equipment assigned to employees or the data stored on or created by that equipment. Datamation reserves the right to access and review any data retained or transmitted by its systems without prior notice, and disclose any information obtained to appropriate parties.

## STANDARDS

### *Collection Limitation*

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

### *Data Quality*

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

### *Purpose Specification*

The purposes for which personal data is collected should be specified at the time of collection.

### *Use Limitation*

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified at the time of collection, except:

- With the explicit consent of the data subject; or
- By authority of law

### *Security Safeguards*

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

### *Openness*

There should be a general policy of openness about developments,

practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of its use, as well as the identity and location of the person responsible for safeguarding the data.

## ***Individual Participation***

All employees and customers have the right to:

- Obtain or confirm whether or not Datamation has data relating to him/her;
- Have data relating to him/her communicated:
- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him/her;
- Be given reasons if a request made is denied, and to be able to challenge such denial; and
- Challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended

## ***Accountability***

The person(s) responsible for collecting, transferring, and storing personal data should be held accountable for complying with the principles stated in the above standards.

## ***Monitoring***

All data systems remain the property of Datamation. There is no personal right of privacy maintained for any electronic equipment assigned to employees or the data stored on or created by that equipment. Datamation reserves the right to access and review any data retained or transmitted by its systems without prior notice, and disclose any information obtained to appropriate parties.

## ***Relevant Laws***

Relevant laws prevailing in the country should be used, if needed, to protect the information.



## INTRODUCTION

This Standard is intended to address the conflict of duties issues which could arise from user access administration within main business applications and IT department. This section is intended for managers and supervisors authorizing user access requests, and for system administrators who are responsible for granting user access within business applications.

There are combinations of transactions within any business application which, when granted within the same user profile, increases the risk of accidental or deliberate modification or misuse.

The following matrices represent a “best possible” scenario. Strict adherence to the rules contained in the matrices may not be possible in some cases due to limited resources. However, these rules should be kept in mind when granting access rights to users. The matrices are only a representative sample for segregation of duties and do not cover all possible combinations where issues may exist.

## POLICY STATEMENT

Segregation of duties must be maintained between incompatible functions in order to minimize the potential for errors and fraud.

## STANDARDS

### *Segregation of Duties*

For each transaction within the business application, there should be adequate segregation of duties between the person authorizing the transaction (usually a supervisor or manager) and the person entering the transaction. It is also necessary to have adequate segregation between the person entering the transaction and the person validating it (usually a supervisor or manager). For example, the person authorizing a customer’s credit limit should not be the person adding that data to the system. Also the person adding the information should not be the one who reviews or verifies those transactions for validity.

All employees capable of authorizing or assigning access rights are required to comply with the basic principles of conflict of duties, as contained in this document.

### *Compensating Controls*

Compensating controls must be put in place in the event that a user account contains conflict of duties issues.

## RESPONSIBILITIES

Managers and supervisors are responsible for:

- Ensuring that user access requests are reasonable and

- necessary, and are correctly authorized
- Verifying that user access requests do not create unnecessary conflicts of duties within the business environment
- Establishing compensating controls to reduce the impact of conflicts of duties
- Periodic (annual or biannual) reviews of user access rights, to ensure privileges are necessary and current

Application administrators are responsible for:

- Ensuring user access requests are correctly authorized and reasonable
- Informing managers and supervisors of any conflicts of duties arising from their user access requests within the application
- Providing information to managers and supervisors to facilitate the periodic (annual or biannual) review of application user access.

## Matrix 1. General Ledger

This matrix shows which disciplines should be kept separate from other disciplines in a well-regulated business environment. An "X" in a box indicates a Conflict of Duties between the horizontal and vertical fields.

	<u>gg</u>		
General Ledger Postings		X	X
Review of Daily Ledger Postings	X		
GL Master Record Maintenance	X		

### Definitions:

<b>General Ledger Postings</b>	Creating and inputting of routine or manual journal vouchers and reversals, rolling of period-end totals, period reporting and opening new period procedures.
<b>Review of Daily Ledger Postings</b>	Verification of daily or weekly journal vouchers by a supervisor or manager.
<b>GL Master Record Maintenance</b>	Additions or changes to chart of accounts, assignment of document and batch number ranges, and mapping of financial information to Company financial reporting structures.

NOTE: This matrix reflects segregation of duties best practices, and it may not be possible to enforce these guidelines in all situations. Ensure that compensating controls are established and adhered to in cases of non-conformity.

## Matrix 2. Accounts Receivable

This matrix shows which disciplines should be kept separate from other disciplines in a well-regulated business environment. An "X" in a box indicates a conflict of duties between the horizontal and vertical fields.

Customer Data Maintenance		X		X	X	X	X
Billing	X		X	X		X	X
Delivery / Distribution		X		X	X	X	X
Sales Order Management	X	X	X		X	X	X
Process Incoming Payments	X		X	X			X
Customer Credit Management	X	X	X	X			X
Credit Issuing	X	X	X	X	X	X	

### Definitions:

<b>Customer Data Maintenance</b>	Updating of customer master data, inclusive of credit information.
<b>Billing</b>	Processing of customer invoice documentation.
<b>Delivery / Distribution</b>	Picking and expediting of goods to customer as per sales order pick lists.
<b>Sales Order Management</b>	Annual price change master updates, sales order inputting and maintenance.
<b>Process Incoming Payments</b>	Accounts receivable, including cash receipts and check deposits, posting to accounts and reconciliation.
<b>Customer Credit Management</b>	Assessment of customer credit worthiness, authorization and updating of credit limits, payment terms and customer price information.
<b>Credit Issuing</b>	Authorization, issuance and allocation of customer credit notes.

NOTE: This matrix reflects segregation of duties best practices, and it may not be possible to enforce these guidelines in all situations. Ensure that compensating controls are established and adhered to in cases of non-conformity.



**Matrix 3.**  
**Accounts Payable**

This matrix shows which disciplines should be kept separate from other disciplines in a well-regulated business environment. An "X" in a box indicates a conflict of duties between the horizontal and vertical fields.

- Vendor Master Data Maintenance
- Vendor Invoice Processing
- Payment Processing
- Purchasing Activities
- Goods Receiving

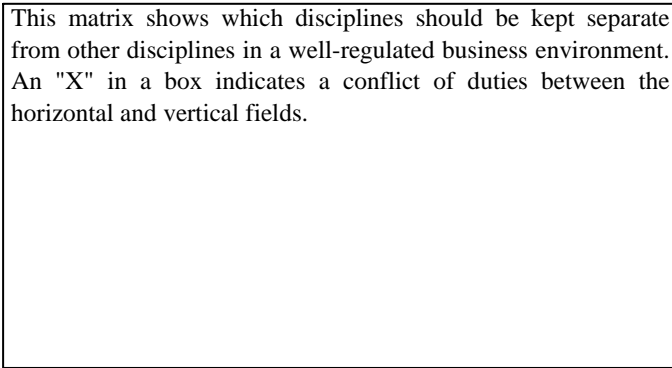
**Definitions:**

- Vendor Master Data Maint.** Authorizing and updating of vendor data, including terms of payment and contact information.
- Vendor Invoice Processing** Validation and inputting of vendor invoices usually matched to purchase orders.
- Payment Processing** Validating Invoices, posting to accounts, issuing debit memos, processing electronic payments and checks.
- Purchasing Activities** Vendor approval, requisition approval; purchase order management, vendor data maintenance.
- Goods Receiving** Physical handling and checking of incoming goods, and booking in of the received / rejected amounts.

NOTE: This matrix reflects segregation of duties best practices, and it may not be possible to enforce these guidelines in all situations. Ensure that compensating controls are established and adhered to in cases of non-conformity.

## **Matrix 4.** **Payroll and Human Resources**

This matrix shows which disciplines should be kept separate from other disciplines in a well-regulated business environment. An "X" in a box indicates a conflict of duties between the horizontal and vertical fields.



HR Employee Master Data

HR Daily Management

Payroll Employee Master Data

Payroll Period Input

### **Definitions:**

#### **HR Daily Management**

Inputting of HR employee dynamic data (such as sickness absences, vacation days and training).

#### **HR Employee Master Data**

Inputting of HR employee static data (such as personal information and duties).

#### **Payroll Employee Master Data**

Inputting of Payroll static data (such as personal information and wage rates, tax and pension).

#### **Payroll Period Input**

Inputting of Payroll dynamic data (such as hours worked, vacation days and sickness leave).

NOTE: This matrix reflects segregation of duties best practices, and it may not be possible to enforce these guidelines in all situations. Ensure that compensating controls are established and adhered to in cases of non-conformity.

## Matrix 5. Materials Management

This matrix shows which disciplines should be kept separate from other disciplines in a well-regulated business environment. An "X" in a box indicates a conflict of duties between the horizontal and vertical fields.

Materials Master Maintenance  
 Goods Receiving  
 Inventory Management  
 Sales Order Management  
 Manufacturing & Production  
 Delivery / Distribution  
 Purchasing Activities

### Definitions:

<b>Materials Master Maintenance</b>	Authorization and master updates of parts records.
<b>Goods Receiving</b>	Physical handling and checking of incoming goods, and booking in of the received / rejected amounts.
<b>Inventory Management</b>	Management of logical / physical stores, goods movements and stock bookings, excluding inventory checks.
<b>Sales Order Management</b>	Authorization and updating of Sales Orders, including schedules and EDI downloads.
<b>Manufacturing &amp; Production</b>	Any manufacturing or production activity, including factory order management or manufacturing scheduling.
<b>Delivery / Distribution</b>	Picking and expediting of goods to customer.
<b>Purchasing Activities</b>	Vendor approval, requisition approval; purchase order management, vendor data maintenance.

NOTE: This matrix reflects segregation of duties best practices, and it may not be possible to enforce these guidelines in all situations. Ensure that compensating controls are established and adhered to in cases of non-conformity.

## Matrix 6. Information Technology

This matrix shows which disciplines should be kept separate from other disciplines in a well regulated Mainframe environment. An "X" in a box indicates a conflict of duties between the horizontal and vertical fields.

Analyst / Programmer

Application Input

Operator / Librarian

Database Administrator

Security Administrator

System Programming

Quality Assurance

### Definitions:

<b>Analyst / Programmer</b>	Interpreting user needs and determining applications to satisfy user requirements; maintaining production systems.
<b>Application Input</b>	Inputting of information through an application into application data files.
<b>Operator / Librarian</b>	Performing of everyday computer operations, maintaining systems and peripherals, including removable media management and storage.
<b>Database Administrator</b>	Designing and administering of application data files, usually residing between the application and the operating system.
<b>Security Administrator</b>	Maintaining security and access to files and resources, violation monitoring and reviewing procedures for improved safety.
<b>System Programming</b>	Maintaining of non-application specific system software, including operating systems.
<b>Quality Assurance</b>	Testing and verifying of programs and changes for adherence to standards and functionality.

NOTE: This matrix reflects segregation of duties best practices, and it may not be possible to enforce these guidelines in all situations. Ensure that compensating controls are established and adhered to in cases of non-conformity.

### **INTRODUCTION**

Disaster Recovery Planning involves the advance planning and arrangements necessary to minimize risk by ensuring the ability to recover time sensitive systems, applications, information and business functions in the event of an interruption or disaster. Disaster Recovery Planning also involves defining, recommending, implementing, testing and administering recovery strategies.

### **POLICY STATEMENT**

It is the ultimate responsibility of the owner of business information to ensure that the recovery and contingent processing of such data is possible through tested and effective backup procedures, recovery planning and contingency processing capabilities. This will increase the ability to recover critical processes and restore critical data in a timely and cost-effective manner.

### **STANDARDS**

Individual Business Recovery Plans must exist for all information processing systems that support critical business functions. Location management must test the plan annually. Location management is also responsible for reviewing and maintaining the plan on an annual basis or when any major change(s) occurs within the IT systems or configurations. The plan(s) must address a situation from partial to total loss (worst case) of a location to ensure the ability to recover and restore IT information, as well as, critical business information. The extent of detail required for each plan will depend on each of the location's critical functions and system restoration capabilities.

### **OBJECTIVE**

The objective of this policy is to:

- Establish alternative strategies to recover critical Company information processing systems.
- Provide guidelines for ensuring the protection and recovery capabilities of Company information in accordance with Datamation's Information Security Policy and Standards.
- Ensure that necessary data can be recovered and processed so that critical business functions can be re-established.
- Provide a methodology for ensuring plans are developed, tested and maintained to minimize any inconvenience or interruption in the ability to continue operations and service the customer.
- Provide a means for situation assessment.
- Establish a methodology for ensuring notification to the appropriate management and support areas in the event of an interruption to operations.
- Establish a methodology for communicating emergency situations to affected employees, clients, customers, and agencies etc.

## RESPONSIBILITIES

### Location Managers

Managers are responsible for business continuity controls and must ensure a secure, recoverable environment that protects IT assets, and provides continuity for the critical business functions that they support. They will approve the recovery plans for their business needs once developed, and thereafter each time the plan is updated.

## THE DISASTER RECOVERY PLAN

The plan should address the following:

- Identification of critical applications and processes.
- Identification of minimum recovery hardware configuration.
- Identification of required software and platforms.
- Prioritizing restoration of applications and verification steps to be performed prior to bringing up further applications.
- Target recovery times for each mission critical function as well as normal service functions.
- Actions to be taken during the four phases of business resumption:
  1. Response (initial action following a disastrous event).
  2. Resumption (establishing the alternative processing site and begin processing time-sensitive business functions).
  3. Recovery (resume processing for less time-sensitive business functions).
  4. Restoration (returning to the original processing site).
- Identification of critical personnel and event notification information.
- Descriptions of how to acquire necessary resources, such as vendor information, temporary employees and supplies.
- Access requirements concerning who is authorized for declaring a disaster, entering the off-site storage facility, gathering recovery resources, or accessing the location after police/fire/detectives have isolated the area.
- Persons authorized to purchase, what they can purchase and authorized spending limits.
- Security issues such as guards and premises protection.
- Communication needs, such as who will address the media in a disaster situation and what employees should **NOT** say to any outside person at this time.

Additionally, the plan should include the following information:

- Notification procedures for employees, vendors and customers.
- Teams, team leaders and contact numbers.
- Action plans for each team (concise step-by step descriptions of actions required).
- Detailed instructions - for Disaster Recovery Procedures and Contingency Procedures.

- Network documentation including telecommunications.
- Up-to-date equipment and software inventory by location.
- Building plans such as air, water and electrical system mappings.
- Evacuation procedures including safe meeting areas.
- Vendor agreements.
- Data classification sheets.
- Contingency plan.
- Vendor contact list.
- Key customer contact list.
- Maintenance schedule.
- Test/exercise schedule.

### **BACKUP/DATA RECOVERY**

Backup and recovery procedures and practices provide a means to save and restore data for all data processing systems including mainframes, servers and workstations. It is the ultimate responsibility of the owner of the data and the systems support staff to ensure that the backup/recovery process is accurate, effective and well documented for recovery purposes. Failure to do so could result in the unrecoverable loss of critical information if a disruptive event occurs.

The frequency of backup information should be determined based on the criticality of the data, the system, location and departmental needs.

A routine schedule for off-site rotation of backup information must be established. Depending on the threat of a regional disaster, the off-site location should be outside of the regional area to avoid total loss of information.

The following backup information should always be available in current status to business users:

- Historical and current system processed information required by law.
- Copies of current versions of the operating system and other significant software used within the organization. This software must be stored off-site unless compatible versions are easily available and customizing/reconfiguring is a minor task.
- Priority listings concerning the restoration of applications in a logical order based on sequences dictated by the system or by management decision. These decisions are made jointly by IT operations, applications managers and business users and should be reviewed annually.
- Maximum expected time which would be required to complete the installation of replacement hardware and software should be

clearly stated (recovery lead times).

- Equipment and network layouts (network and software configuration diagrams) and any other information vital to restoration of the current system or necessary for setting up a new system(s).

Non-system related backup information that is very important, and should be held at off-site locations, includes, but is not limited to:

- Hardware and software inventory, including serial numbers and detailed information that would be useful for identifying needed items such as makes, model numbers, engineering release levels and types of equipment used to process transactions. This listing should also include alternatives to equipment in case of unavailability.
- Copies of current operational manuals and procedures or access to (i.e., from other site, vendor or offsite data storage).
- Important legal/originals of critical documents.
- Unique critical supplies.
- Vendor listings that could be used to expedite the replacement of hardware, software or important supplies that need to be purchased quickly.
- Important business forms and documentation such as purchase orders, invoices and blank checks that may be required in a disaster situation.
- Information particular to the functionality of a department that would be vital for the continuation of critical business processes.

Backup requirements and recovery strategies for transmitted and received data (electronic media) must be considered.

Review and updating of all items maintained in an off-site storage area should take place on an annual basis.

### **TESTING AND MAINTAINING THE PLAN**

It is essential that Disaster Recovery Plans be tested on an annual basis. If an agreement exists for alternative sites, it is desirable that exercising take place utilizing the actual recovery facility. After an exercise, all recovery personnel are responsible for submitting a written report indicating problems encountered and plans for resolution. The plan should be updated to reflect those recommendations.

A management review of the plan should take place at least annually or more frequently when significant changes are made to the applications, hardware or software at a location.



## **COMMUNICATION/ AWARENESS/ DISTRIBUTION**

Each employee should be aware of their role and responsibilities in a recovery effort and should participate in plan tests when possible.

All primary and alternate key personnel responsible for participation in the business recovery should maintain a copy of the plan, both at work and at home. (Depending on their assigned roles, it may not be necessary to distribute the entire plan to all individuals.)

Datamations Internal Audit will also maintain a current copy of all Disaster Recovery Plans in the Company.

## **ALTERNATIVE SITES**

In the event that a facility is damaged and inaccessible or a business interruption occurs that requires relocation of the business, then alternative locations would be required. The capacity of an alternate location/recovery site should meet the minimum needs required to address critical processing functions. These needs would be based on the alternative processing strategy, the time required to recover the critical business functions and options for alternate/recovery sites.

## **Service Providers**

Where no Company strategy exists and it is beyond reasonable cost to justify redundancies, agreements must be made with vendors who offer services such as temporary and permanent hardware/software replacement, office space/furniture, and supplies, etc., in advance. This will guarantee quick response in a disaster situation. The distance of recovery sites from a Datamation location is important to consider since key employees are expected to be present for both actual recovery and testing.

Annually, a review of recovery service vendor contracts must be done to ensure compatibility. Testing system recovery will ensure present system configurations are recoverable at the alternate computer site and that operating systems and business function software is appropriately backed up. In addition, the number of workspace areas should be analyzed to avoid deficiencies at time of need. Other contractual considerations that must be given are options to void contracts when special circumstances exist, i.e. acquisitions, sale of existing business, etc

## **RISK ANALYSIS**

A risk analysis is the process of identifying risks, assessing the critical functions necessary to continue operations, defining the controls that are in place to reduce exposure, and evaluating the cost for such controls. The risk analysis often involves an evaluation of the likelihood of an occurrence. The risk analysis will be performed on computer/network environments to identify

and evaluate risks and determine any disaster mitigation requirements. The risk analysis is generally a collaborative effort of various departments including IT, Facilities Management, Infrastructure Management, General Management, Internal Audit, along with any public utilities and services which support the Company.

### **EXISTING SYSTEMS**

Evaluations of existing systems to determine whether the system complies with the Company policy will be performed by DM's Internal Audit. If not in compliance, the location is responsible for determining recovery strategies and documenting a recovery plan that must be tested and maintained annually.

### **NEW SYSTEMS**

Recovery considerations must be provided within the project charter for all new/upgraded IT systems intended for critical business functions. DM's Internal Audit, along with business units and IT development areas, will ensure that any system/application being considered for purchase is evaluated for compliance this policy.

## **INTRODUCTION**

The purpose of this policy is to establish management direction and requirements to ensure the appropriate protection of Datamation information handled by computer networks.

This policy applies to all employees, contractors, consultants, temporaries, and third parties who access Datamation computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by Datamation.

The objective is to provide requirements, conditions and expectations to be applied and practiced concerning Company network systems, equipment, connectivity and management.

## **POLICY STATEMENT**

All locations that are connected to the Datamation Wide Area Network (WAN) must secure their network according to Information Security Policies and standards. These networks must be secured to ensure confidentiality, integrity and availability of the information that passes across the network and systems that reside on the network.

## **STANDARDS**

### ***Configuring Networks***

The network must be designed and configured to deliver high performance and reliability to meet the needs of business while providing a high degree of access control and range of privilege restrictions. All network infrastructures must follow not only company standards.

Networks must be documented to ensure the access points, points of failure and overall layout is understood. Network documentation includes network diagrams, procedures, standards and guidelines. This documentation must be kept up-to-date to reflect any significant changes in the network.

Care should be taken to minimize the protocols (IPX, IP, etc.) on the local area network and communications across the wide area network. Protocol convergence can assist in network management, reliability and security enhancement.

### ***Managing and Monitoring the Network***

Suitable qualified staff are to manage the organization's network, and preserve its integrity in collaboration with individual system owners. LAN and WAN management must be coordinated with Company Information Technology to ensure IT Standards are being followed and that appropriate methodologies, products and tools are being

used.

The use of network sniffers or other monitoring software/hardware must only be used to monitor and manage the network to ensure availability as well as to identify and resolve network related problems. Sniffers must not be utilized to intercept or capture information as it travels the network. Only authorized personnel within IT are permitted to utilize sniffers in accordance with their job responsibilities.

### ***Connecting to the Network***

Only authorized users are permitted to connect to any Datamation company network. Unused network jacks should be disconnected when not actively used to prevent unauthorized users from accessing company networks. IP addresses must only be assigned to authorized users. Dynamic addressing (DHCP) for end-users and static addressing for servers and dedicated equipment are recommended. Static IP addressing for users may be used when the business infrastructure has a business and technical justification. Where static IP addresses are utilized, users must only obtain addresses from the appropriate IT management and are not permitted to assign their own address.

### ***Accessing the Network Remotely***

Remote access to all Datamation networks and resources may be permitted providing authorized users are authenticated, privileges are restricted, and data is encrypted across any public network (e.g., the Internet). This access must be approved in advance by the associate's manager or information owner. Such remote access is not a universal fringe benefit and may be revoked at any time for cause including unsatisfactory performance and non-compliance with security policies. Current remote access solutions consist of:

- Centralized Dial-up using strong authentication
- Dial-in and replication
- Virtual Private Network (VPN) with strong authentication, up-to-date virus protection and personal firewall (See Remote Access Policy & Acknowledgement Agreement for additional

information)

Associates must not establish connections with any third party, external network, Internet Service Provider (ISP) or other external networks for the transmission of company data unless this arrangement has first been approved by Information Security. See Gateway Standards for additional details.

### ***Third Party Access to Datamation Internal Networks***

In strictly controlled situations, Datamation does allow third parties to access Datamation internal networks and connected computer systems. Both the information owner and the project manager in charge of the third party's work must agree in writing to such access before being established. The decision-making process for granting such access includes consideration of the controls on the systems to be connected, third party's security policies, and results of a background check. Privileges for such third parties must be strictly limited to the system facilities and information needed to achieve predefined business objectives. These access privileges must be reviewed every six months by the relevant project manager to determine whether they need to be continued. Appropriate contracts and non-disclosure agreements must exist prior to providing any connectivity or access.

### ***Vendor Access***

Third party vendors that have sold Datamation hardware, software, or communication services are not automatically granted repeated access to Datamation internal computers and/or networks. They must go through the approval process described in the previous paragraph and comply with the company policies and standards.

Temporary remote access privileges for vendors may be enabled by a systems administrator without going through the approval processes. This temporary access must be granted only for the time period required to accomplish approved tasks (one day or less). This temporary access must be provided by positive identification of the vendor personnel before the connection is established, as well as logging of all activity while the connection exists.

### ***Compliance Statement***

All third parties wishing to remotely access Datamation internal computers or networks must sign a compliance statement prior to being issued a user-ID. If a third party already has a user-ID, a signature must be obtained prior to receiving a renewed user-ID. A signature on this compliance statement indicates the involved user(s) understand and agree to abide by Datamation policies and procedures related to computers and networks. Datamation retains the right to periodically audit third parties who have access to Datamation computers and networks to ensure compliance with

this and other policies and requirements. Contracts, which include non-disclosure-agreements, privacy statements, and/or service level agreements, must also exist between entities prior to authorizing access.

## *Wireless Networks*

Wireless networks that are deployed must use a level of encryption or virtual private network (VPN) to protect against unauthorized interception and access. Additionally, peer-to-peer or extensible authentication should be used to ensure the end user or computer is authorized to access company networks. The following controls must be implemented if wireless is considered:

- Change the SSID (network name) from default. Also, if possible, prevent the broadcast of this SSID on the network.
- MAC Address restrictions
- 128-bit Wired Equivalent Privacy (WEP) encryption
- EAP Authentication
- Mutual Radius Authentication for each user of a wireless device.
- Dynamic WEP key (should be changed every four hours or less) and generated upon successful authentication.

Where wireless networks are in consideration for deployment, Information Security must be involved to ensure appropriate security controls are implemented to mitigate the risk of unauthorized access and loss of data integrity. Information Security must be made aware of all wireless networks and they must maintain a record of all wireless access points deployed throughout Datamation.

**Note:** A recommended solution is the Cisco Aironet access point and wireless cards capable of LEAP while ensuring all the security features defined within this policy and standard.

## *Network Services*

Only network services (ftp, ssh, http, etc.) absolutely necessary for business shall be enabled on computer systems and network devices that reside on Datamation networks. When sensitive services are needed, consider implementing access controls such as port filtering, firewalls or tcp wrappers to control who can access and use these services.

When using network services, especially on untrusted networks, a risk assessment must be performed to ensure the information integrity remains intact. Several network services are considered unsecured protocols, meaning anyone could view the contents of a message as it passes along a network. This includes the ability to view the user ID and password, resulting in the potential modification and disclosure of company information. The most commonly used unsecured protocols include telnet, ftp, http, and smtp. If these protocols are

being used, the information owner must understand accept the risks or seek alternative protocols to secure the information as it traverses the network. Protocols such as https and ssh are common replacement for http and telnet.

### ***Segregation of Network***

Networks that are non-company owned and operated must be separated by a firewall or other access control mechanism. See Gateway Standards for further detail. Contracts, which include non-disclosure-agreements, privacy statements, and/or service level agreements, must exist between entities prior to establishing network connections. Only those services and applications absolutely required will be permitted between the non- company owned networks.

### ***Data Exchange and Encrypted Links***

Whenever a computer network connection is established with a Datamation internal computer or network from a location outside an official Datamation office, and whenever this connection transmits or is likely to transmit company sensitive information, the link must be encrypted. Such encryption must be accomplished only with systems approved by Information Security.

### ***Modem Usage***

Access into Datamation company networks using dial-up will be in addition to normal security systems and will not preclude the entry of user Ids and passwords normally required by the system being used. For example, users will be provided an additional form of authentication to perform such activities.

The use of dial-up access directly into a personal computer, business system or local area network is prohibited unless it is routed through the centrally managed dial gateways or modem pools. Where modems are absolutely necessary on company resources and do not go through a centrally managed gateway, the use of the modem must be documented and provided to Information Security. Those modems must be disabled or turned-off when not being used.

Modems in or connected to office desktop PCs are not permitted. Home based, mobile and/or telecommuting microcomputers are an exception to this rule. Unless a dynamic password system is installed, associates with home based, mobile, or telecommuting PCs must not leave modems in auto-answer mode, with communications software enabled, such that in-coming dial-up calls could be received.

### ***Outbound Connections***

Computer network connections initiated from inside an official Datamation office, and connecting to an external network or computer, do not need to employ extra access control systems. These connections must however be routed through dial-up modem pools, Internet firewalls, and other systems expressly established to provide

secure network access.

If a user must utilize a dial-up line and modem, the user's connection to the company network must be disconnected during modem/dial-out usage.

## ***Default to Denial***

If an Datamation computer or network access control system is not functioning properly it must default to denial of privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.

## ***Remote Control***

Remote control (PC Anywhere, Terminal Services, etc.) access to workstations or servers *may* be permitted on a strictly limited basis after being approved by Information Security. The Information Security department will perform a risk assessment to determine whether the requested remote control connection is acceptable. This access will only be provided using an IP address after an initial network connection is made through a modem pool, Internet firewall or VPN. The Company requirements for user authentication, encryption and information integrity as outlined in those policies will also apply.

## ***Radio and Cellular Technology***

Portable phones using radio technology as well as cellular phones must not be used for data transmissions containing Datamation Private, Critical and/or Financial information unless the connection is encrypted. Likewise, other broadcast networking technologies--such radio-based local area networks--must not be used for these types of Datamation information unless the link is encrypted. Such links may be used for electronic mail as long as involved users understand that the transmissions must not contain readable Private, Critical and/or Financial information. Similarly, Associates must not discuss Private, Critical and/or Financial matters on cordless or cellular phones employing a regular voice connection, unless this connection has been encrypted with technology approved by the Information Security Department. Phones using digital transmission rather than traditional analog transmission protocols (such as PCS and Verizon) are not considered to be encrypted for purposes of this policy.

## ***Shared File Systems***

The establishment of a connection between any external computer or network and a Datamation internal computer or network must not involve the use of shared file systems such as NFS (Network File System). This will help to ensure that sensitive information is not inadvertently disclosed to unauthorized persons. An exception may be made if Information Security approves the configuration prior to usage and appropriate access controls and monitoring solution are established.



## ***Logs for Externally Connected Systems***

All Datamation computers and networks which interface to external networks must maintain system logs which indicate the identity and activity performed by each user who gains access to these systems. These logs must indicate the time of day, the date, the user-ID employed, any special privileges utilized, and other details associated with all connections (whether permitted or denied). Systems administrators must regularly review these logs or use automated intrusion detection systems to immediately inform them of suspicious activity.

## ***Unauthorized Access and Network Browsing***

Users are prohibited from gaining unauthorized access to any information system or network to which they have not been expressly granted access. Users are also prohibited from in any way damaging, disrupting, or interfering with the operations of multi-user information systems to which they are connected. Likewise, users are prohibited from capturing or otherwise being in possession of passwords, encryption keys, or any other access control mechanism that has not been expressly assigned to them.

Users must not browse through Datamation computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job is not considered browsing. This statement on browsing does not apply to external networks such as the Internet.

## ***Changes to Datamation Networks***

Changes to Datamation internal networks include loading new software, changing network addresses, reconfiguring routers, adding dial-up lines, implementing wireless technology, adding new infrastructure items including, but not limited to routers, switches, hubs, network cabling and fiber optics and the like. With the exception of emergency situations, all changes to Datamation computer networks must be documented and must be approved in advance by the Information Technology Department. Emergency changes to Datamation networks must only be made by persons who are authorized by the Information Technology Department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. Additionally, associates deploying new systems must take the appropriate action steps to ensure each system is configured securely. Information Security can also be contacted for assistance.

## ***Installation of Communications Lines***

Associates and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not first obtained approval from appropriate Information Technology management.

## ***Establishing New Business Networks***

Associates are prohibited from using the Internet or any other external network to establish new or different business channels unless Information Technology management, executive management and Legal Counsel have approved this in advance. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.

## ***Disclosure of Systems Information***

The internal addresses, configurations, and related system design information for Datamation computers and networks is confidential and must not be released to third parties who do not have a demonstrable need-to-know such information. Likewise, the security measures employed to protect Datamation computers and networks is confidential and should be similarly protected.

## ***Security Tools***

Unless specifically authorized by Information Security, users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, test or compromise information systems security. Examples of such tools include those which defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files. Similarly, without this type of approval, users are prohibited from using “sniffers” or any hardware or software tool, which monitors the traffic on the network or the activity on a computer.

## INTRODUCTION

### Background

Datamation's presence on the Internet has grown immensely over the years and continues to grow as technologies evolve and businesses adapt. As a result, there is an increased need to manage security risks at the gateway since this is the entry point into the Company network and first line of defense.

### Purpose

The purpose of this document is to define the standards and guidelines for implementing, managing and monitoring gateways based on security considerations to protect the company's network and information.

### What's a Gateway?

A gateway is typically thought of as a connection or access point to the Internet. Datamation defines a gateway as any TCP/IP based connection between a trusted and an untrusted network. An untrusted network consists of the Internet, third parties (suppliers, partners, customers, joint ventures, etc.) and potentially disconnected Datamation locations.

### Decision Makers

The Information Security group is ultimately the decision-maker regarding gateway implementations. Information Security will work with the business owner and IT management to ensure adequate design, deployment and management of the gateway.

## POLICY STATEMENT STANDARDS

Only authorized and approved gateways are permitted on the Datamation Wide Area Network (WAN). The standard hardware and software must be used when deploying gateways throughout the company. Any exceptions from the standard must be approved by Information Security. The gateways must also be managed and monitored in accordance with company policies and standards.

## *Hardware and Software* **Firewall**

CISCO FireWall-1 is the standard firewall software within Datamation. Depending on the location and requirements, FireWall must meet with specifications that meet business and technical requirements.

A typical FireWall instance requires a firewall module to protect each gateway. The firewall module communicates with a management console for configuration and logging. Each gateway requires the firewall module and multiple firewall modules can communicate to one management console. The firewall management console must run on a secured Windows 2000 machine.

## **Proxy Server**

Post Master is the standard content filtering software. This software proactively blocks and/or monitors access to inappropriate and unproductive content on the Internet.

Post Master is typically installed on a proxy server or a gateway appliance. The current proxy server standard is Microsoft Proxy Server, but another proxy server such as Microsoft ISA server can be used if approved by Information Security.

## **Virus Scanning**

Virus scanning should be implemented at all major gateways, which support company web and mail applications. McAfee WebShield is the standard gateway anti-virus software and can be run on any appliance that can handle the throughput without degrading network performance.

## *Management and Control*

## **Firewall Architecture & Design**

Every gateway must employ a firewall to ensure Datamation's network and information is protected. However, there are several architectures that could be implemented based on the business requirements. These options include the implementation of demilitarized zone ("DMZ") or a straight through connection. A DMZ is typically used to isolate Internet accessible servers off the private internal network. For example, web, ftp and mail servers generally sit inside the DMZ. Depending on the business and application requirements, there may be a need for multiple DMZ's. Broadband connections will typically not have a DMZ, rather they will use a straight through architecture to filter access to the Internet and prevent access to the sites' local area network. See diagrams for architecture scenarios on pages 15-14 and 15-15.

### **High Availability & Load Balancing**

High availability may be required based on the business requirements of the gateway architecture. The standard for fail-over is to utilize the VRRP protocol within the CISCO appliances running CISCO FireWall-1. Where fail-over requirements are not established, an agreed tolerable downtime must be established.

Critical web applications may also require the use of a load-balancing device to distribute the capacity across servers or devices within the gateway architecture. When load balancing is required, due diligence must be performed to ensure an appropriate selection is made. Several popular load-balancing devices include F5's Big IP and Cisco Local Director.

### **Management Console**

The firewall management standard is to have multiple firewall modules communicating with one or two management consoles in a geographical area

### **Proxy Server**

A proxy server is required for user access to the Internet. The proxy server must be located inside the firewall and users pass-through this system to access the Internet. The use of a proxy server provides an additional level of security and manageability to Internet access. In addition to the placement of the proxy server, Post Master must be implemented with user authentication to block and monitor access to inappropriate or unproductive content. Caching must also be utilized to alleviate the overhead on the network bandwidth. Within the Post Master software, the following site categories must be blocked at a minimum:

- Adult/Sexually Explicit
- Chat
- Criminal Skills
- Drug, Alcohol, & Tobacco
- Food & Drink
- Gambling
- Games
- Hacking
- Hate Speech
- Hobbies & Recreation

- Personals & Dating
- Remote Proxies
- Streaming Media
- Usenet News
- Violence
- Weapons

**Note:** There may be additional categories added over time, therefore discretion must be used when blocking or allowing categories to ensure personnel are not permitted to access unproductive and offensive sites.

If sites are categorized inappropriately or there is a business reason to access a blocked site, there are two options to resolve the issue. The first is submitting a re-categorization request on the vendor's web site and the second is to add the site to an unblocked list in the SurfControl configuration. In either event, care must be taken to ensure only appropriate web sites are opened. SurfControl should also be setup to download library updates on a nightly off-hours basis.

### **Rulebase and Security Policy**

In order for the firewall to communicate between the trusted and untrusted network, rules must be written that specify what network traffic can pass between the two. Building a solid rulebase is a critical, if not the most critical, step in implementing a successful and secure firewall.

The firewall rulebase and security policy must be designed to ensure adequate protection of the enterprise. The following are guidelines that must be followed when writing the rulebase:

- Keep the rulebase simple and organized to ensure manageability and understanding while reducing potential for improper configuration
- Rules should be designed in top down order
- Commonly used rules will be placed near the top, which will increase firewall performance
- Create a "Stealth Rule" to block any access to the firewalls
- A specific rule must be created for admin and management access to the firewall(s)
- Implied Rules will not be enabled unless there is a specific business requirement and mitigating control mechanism. Rule should be written where necessary to accomplish required functionality
- Admin access will be restricted by an IP addresses on the internal network and utilize encryption

- Drop all traffic and log as the last rule (“Cleanup Rule”)
- Do not log broadcast traffic, rather create a rule that drops/rejects this traffic without logging
- Do not allow wide-open access to the DMZ from inside or outside the company network. Access to the DMZ’s must be on a business need and security measures must be established
- Utilize Network Address Translation (NAT) to mask internal IP addresses from those available to the untrusted network
- Define a “Sneaky Rule”, since the DMZ should almost never communicate with the inside network. This rule must deny, log and alert any traffic from the DMZ’s to the internal network. If traffic is identified, the DMZ has more than likely been compromised

### Security Requirements

The following security requirements are to be implemented on systems within the gateway architecture:

#### Access Control

- All Internet access from the Company network must occur over proxies situated firewall
- Default configuration: unless otherwise specified, services are forbidden (“denial by default”)
- All users are allowed to exchange mail with Internet users
- Anonymous mail (smtp) relays are not permitted
- Split DNS must be used to ensure internal addresses and names are not published or available outside the company network
- Use only “static” routes on the firewall.
- Zone transfers must not be permitted within the DNS configuration of the gateway
- Authorized users are allowed to use outbound www (http/https) and ftp services. If additional services are required for business purposes, the risk must be assessed and approved by management
- Traceroute is not to be implemented through the gateway or firewall to eliminate network mapping risks
- IP Forwarding may not be enabled on the firewall during boot time

- Peripherals (CD/Floppy Drives) must be removed or restricted to eliminate any walkup attacks
- Restrict physical and logical access to the consoles of the firewall and other systems in the gateway architecture

#### Assurance

- Firewall and proxy machines are to be installed as sensitive hosts. All unnecessary services are to be stopped in the operating system. Users should not be able to logon directly to these machines
- The firewall policy, rulebase and configuration must be accurately documented

#### Outbound Services

The following services are permitted from specific internal hosts or users (e.g. via proxies) to the Internet:

1. Email, WWW (http/https), ftp, telnet, ssh
2. DNS (resolve Internet names)
3. News (nntp) must be limited to the business required sites
4. Sensitive files or messages must be encrypted if being sent via email, ftp, http or other unsecured protocols

#### Inbound Services

The following services need to be allowed into a protect DMZ:

1. Email: all users should be able to receive Internet Email, via secured gateways through the Company mail systems
2. WWW: web traffic is permitted to secured hosts on the DMZ and comply with security, business and other IT standards and requirements
3. FTP Servers
4. DNS resolution of gateway machines, not the internal network

Any machines requiring Internet services must be placed on the DMZ and a risk assessment must be performed to ensure the security risks are mitigated to an acceptable level.

#### **Account Management**

Only administration accounts are permitted on the firewall or other devices within the gateway architecture. If user accounts are required, a third party repository must be implemented with strong authentication. Authentication must occur only using secure protocols such as ssh and https. Refer to Chapter One (User Accountability) and Chapter Six (Access Control) for additional requirements.



Default or system accounts must be disabled or the password must be changed. Administrators must utilize unique accounts, where possible, to ensure accountability rather than using generic accounts such as admin, root, etc. Upon termination or change in responsibility of an administrator, the administrative account passwords must be changed immediately. Refer to Chapter One (User Accountability) and Chapter Six (Access Control) for additional requirements.

### **Change Management**

Every rule addition or modification must be documented within the comment field of the firewall. The following information must be included:

- Description of the rule and/or reason for change
- Initials or name of the person making the change
- Date and time of change
- Date and time the initial rule was created

Upon making changes to the firewall rulebase, the policy must be saved to reflect the year, month and day. For example, July 25, 2002 would be depicted in the policy file name as “20020725”. Saving policy changes in this regard easily allows the “roll-back” of the firewall security policy should a problem occur.

A formal or informal risk assessment must be performed to evaluate changes for potential interruptions, performance and security risks. The business owner assumes all responsibility for any modifications to the gateway architecture if a risk exists.

Changes to the gateway architecture, not just the firewall, must be assessed, documented and approved by Information Security.

### **Keeping up-to-date**

A key component to firewall and gateway management is ensuring systems as well as security knowledge are up-to-date. Personnel responsible for the security of the gateway must be current on security issues and news. Mailing lists, websites, professional organizations, etc. are great mediums for staying current with security topics.

Keeping systems patched and updated is one of the most critical aspects of gateway management. The gateway is often under attack from outsiders, therefore it is crucial to stay current on operating system and application patches and releases to ensure the system and company are not vulnerable. There are three key principles when it comes to keeping systems up-to-date:

1. Do not patch problems you do not have. For example, if a server is not running or have installed the daemon for SNMP there is no need to install a patch or update for this service
2. Test and research all patches/upgrades prior to placing into production. This will help to ensure there is minimal impact on any systems or applications running in this environment
3. Review vendor and security advisories to ensure vulnerabilities that affect the environment are identified and mitigated quickly

### **Backup and Recovery**

Once the firewall has been built, the configuration must be backed up and stored according to company policy. The firewall is typically a static configuration; however, a new backup must be performed when the configuration or architecture is modified. Within CISCO FireWall-1, the following information must be backed up:

- Rulebases/Security Policy
- Network objects and properties
- GUI Rules
- User Database
- Static routes
- License Keys for firewall and management modules

There may be additional files required for backup, depending on the installation and configuration of the firewalls.

Other servers, such as proxy, ftp and web, should use normal business and IT standards for backup to ensure successful recovery and reduce downtime. Automated backups should be used whenever possible.

The router configurations must be backed up, as changes occur to ensure successful recovery in the event of systems failure or disaster.

### **Outsourced Management**

A requirement may exist where outsourcing the management of the firewall is the best solution for the business. When outsourcing is the best option, there must be a due diligence process to ensure the most appropriate provider is selected. Upon selection of the provider, service levels, non-disclosure and other contractual arrangements must be established.

Information Security along with the Business Owner are responsible for determining if outsourced firewall management is the best solution. Information Security will manage any projects to identify and select the provider as well as maintain ownership of any such contractual relationships.

## *Monitoring*

### File Systems

The disk space and file systems must be monitored on all systems within the gateway architecture. Disk space must be monitored to ensure there is adequate capacity. Processes must also be established to rotate and truncate log files on a scheduled basis such as bi-weekly or monthly.

### Log Analysis

There are several configurations and analysis that must be performed on the firewall and other component of the gateway architecture. The following are several guidelines regarding log analysis and configuration:

- Detailed logs must be kept on a separate server, if possible. For example, firewall module log information is sent to the firewall management console.
- Dropped/rejected packets, denied connections and rejected attempts must be logged
- Log all errors from routers, firewalls, proxy's and other servers within the gateway architecture
- Log the time, protocol and user name, where applicable, for connections to or through the firewall
- Administrators should look for exceptions to the usual patterns and trends
- Consider using scripts to analyze, query and review firewall and system logs
- Log message into 3 categories
  1. Known to be OK
  2. Known to be dangerous
  3. Unknowns
- Whenever possible, setup alerts to notify administrators via email or pager of unusual events and activity

### Intrusion Detection Systems (“IDS”)

There are two types of intrusion detection systems, hosts and network based. Host based IDS (HIDS) monitors the operating system and configuration of the system while network based IDS (NIDS) monitors traffic patterns. Each IDS system looks for attack patterns, which indicate a potential security event.

NIDS will be used to monitor activity from untrusted networks based on the overall risk and services available. In limited cases, NIDS may not be required due to the architecture and relatively low risks; however, this must be assessed by Information Security. These systems will be placed outside the firewall, inside the DMZ, and inside the firewall to monitor various levels of attacks and activity.

solutions or a multi-vendor approach may be utilized if approved by Information Security. Information Security will be responsible for designing, approving and potentially managing IDS throughout the company.

HIDS should be used on sensitive hosts such as ftp, web and application servers to monitor the system configuration and system level security. For example, HIDS could monitor a web server and notify personnel or prevent inappropriate changes from occurring. HIDS can assist in the identification and prevention of “hacking” activity to the host level.

Within both IDS systems there are several items that must be configured and monitored on a proactive basis. The following are several guidelines for the IDS:

- Ensure IDS signatures are up-to-date. Without the most current signatures or patches, new attacks may not be identified properly
- Consider using products that perform behavioral monitoring in addition to pattern recognition
- Define alerts for scanning events (i.e. port scans, IP half scan, ISS, etc.) to ensure administrations are notified during the enumeration portion of an attack
- Define alerts for critical or high risk events representative of the architecture
- Identify “false positives” and configure the IDS system to minimize these events
- Utilize event propagation on source and destination IP address to limit the amount of events or alerts received

As with any system, administrators should know their environment and the traffic patterns in each. The IDS system will allow for more proactive monitoring of the environment

### **Regular Auditing**

The firewall rulebase and architecture must be audited during initial setup, when changes occur, and at least annually to ensure the highest level of security. Auditing does not necessarily require a formal review by Internal Audit, rather a review by administrators or engineers of the configuration plus additional technical testing to ensure everything is functioning as intended and there are no open security holes. Vulnerability scanning tools must be used during the technical assessment portion of the audit. Upon identification of any vulnerabilities or issues, the architecture and/or configuration must be modified accordingly. A third party should be used to validate the security of the gateway at least every 18 months.

### **Outsourced Monitoring**

Although there are techniques and tools that can be utilized to monitor the gateway architecture, outsourcing of security monitoring is sometimes more effective and efficient due to the number of attacks/events that occur from the Internet. Additionally, outsourcing security monitoring provides 24 x 7 x 365 coverage. Outsourced security monitoring is very popular for larger gateways, which contain web, application, mail, dns and ftp servers.

Information Security is responsible for determining if outsourced monitoring is the best solution. They will also manage any projects to identify and select an outsourced security monitoring provider. Information Security will ultimately maintain ownership of any such contractual relationships.

## *Training and Support*

Primary support for all gateways will be performed by Information Security. In limited instances administration may be delegated or co-sourced to qualified IT personnel at the location.

Personnel whom are responsible for administration and operations of gateways must have appropriate certifications or provided competency to Information Security. Formal training may suffice in lieu of certifications if approved by Information Security.

If a third party is used for management, due diligence must be performed to ensure competency. Service levels that reflect the level of support required by the business and competency of the provider shall be written into contractual obligations for gateway management and/or monitoring.

## *Virtual Private Networks*

A Virtual Private Network (“VPN”) is an encrypted tunnel between two points, typically either two firewalls or a PC and a firewall. Within Datamation, the two types of VPN’s are implemented. The following controls must be implemented on site-to-site or firewall-to-firewall VPNs:

**Note:** Due to export restrictions and regulations within countries that Datamation operates, the laws must be reviewed to ensure compliance in using encryption products.

***Third Party Connections*** When a connection is required to a third party, a firewall must exist between Datamation and the third party. If the connection occurs over the Internet or other public network (i.e. Automotive Network Exchange), a VPN must be implemented. However, if the connection occurs over a private network then the use of a firewall is appropriate.

Any third party connection will only allow the required services and IP addresses to communication. Non-disclosure and other contractual agreements must exist prior to providing any level of connectivity. Logging and monitoring must also occur between this link and administrators of each site must be notified when unusual events are identified.

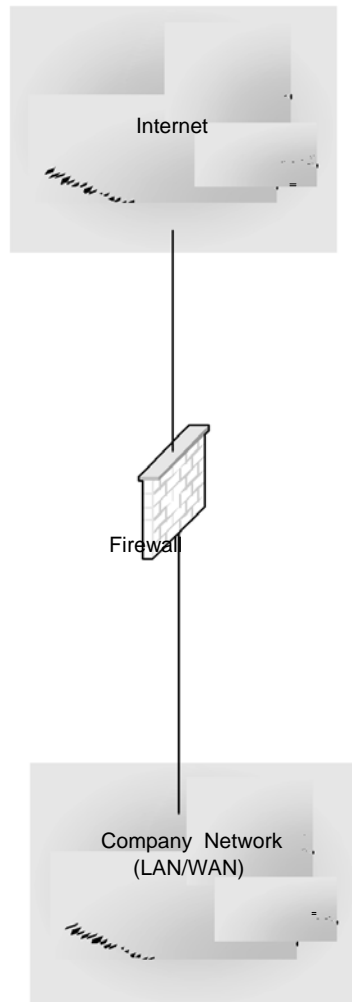
***Exceptions*** Information Security must be involved with the design, deployment and approval of ANY gateway within Datamation. Ultimately, Information Security will maintain ownership of any contractual relationship in this regard.

The Information Security group must also review and approve any exceptions to the standard and supporting policies. These exceptions must be documented.

***Compliance*** Information Security and Internal Audit are responsible for ensuring and monitoring compliance with the policies and standards contained herein. Violations of these standards could result in loss of location connectivity into the Datamation network, civil or criminal liability, and/or possible termination of employment.

Management and users are responsible for complying with the policies and standards contained herein.

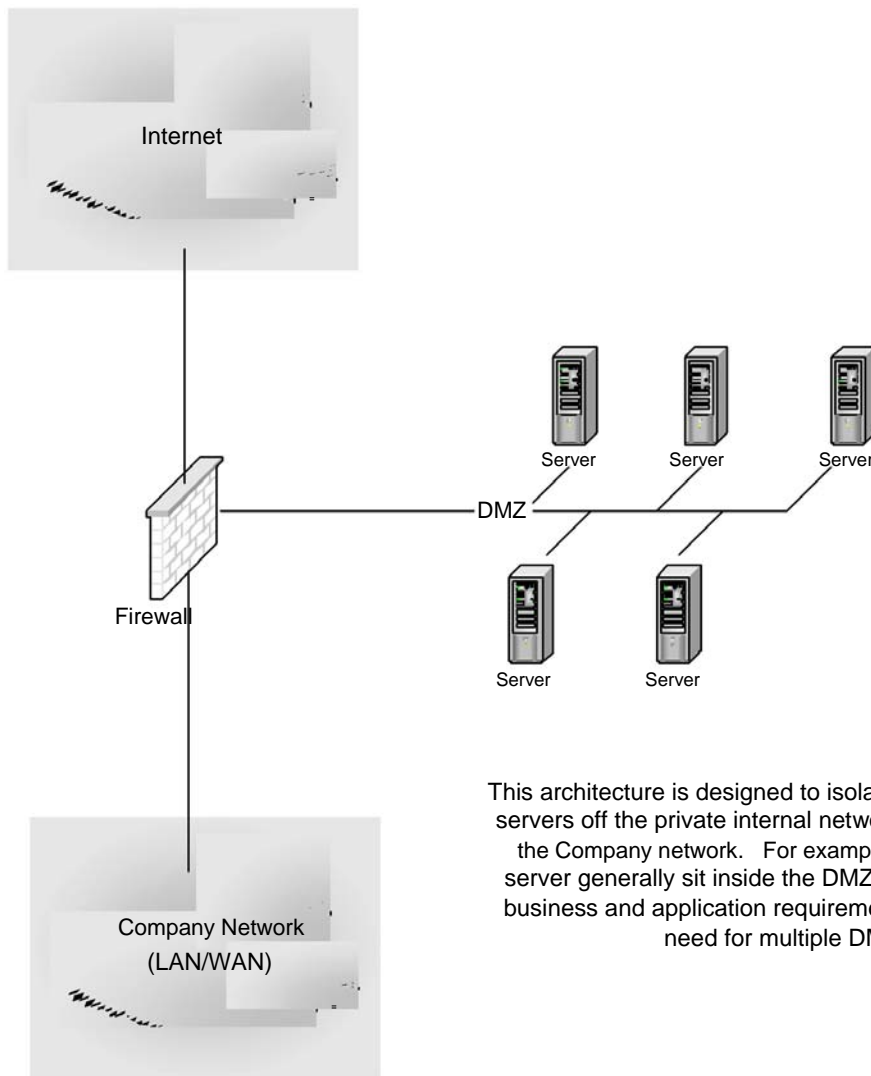
## Straight Through Connection Architecture



This architecture is typically designed for broadband connections. This configuration will be utilized to filter access to and from the untrusted network (e.g., the Internet). No services (i.e. ftp, mail, web) or servers will be available to the Internet in this model.



## Demilitarized Zone Architecture



This architecture is designed to isolate Internet accessible servers off the private internal network as well as protect the Company network. For example, web, ftp and mail server generally sit inside the DMZ. Depending on the business and application requirements, there may be a need for multiple DMZ's.

## INTRODUCTION

This Policy and its Standards are developed to offer sound security practices to prevent losses of laptops and the sensitive information on Company laptops.

## POLICY STATEMENT

Company-owned laptops **must** be secured at all times to prevent loss of the computer and the sensitive information contained within.

## STANDARDS

### User Considerations

Don't leave your laptop in an unsecured office or on a desktop when leaving for the day. Take the unit with you or secure it in a lockable office or lockable drawer out of sight.

When going through airport security, wait until just before you step through the metal detector to place your computer on the belt for x-ray. Don't allow others to step in front of you. This is a scheme used by teams to pick up laptops.

Never leave your laptop inside your vehicle when you go to a meeting. Place it in the trunk out of sight or take it with you.

Keep your laptop with you in the lobby when you are checking into a hotel. Place the case on the floor between your legs, or step on the strap with your foot. Don't get distracted by strangers making conversation.

Don't leave your laptop in your hotel room out in the open. Take it with you when you leave if possible, or conceal it inside your luggage bag, under the bed out of view, or at the front desk in a safe deposit box.

Report the loss of any laptop immediately to Company Security and the local police. Keep a record of the unit serial number. This information can be quickly entered into the police database and improve the chances for the unit to be recovered in the future. This will also allow access to any Company networks to be quickly deleted.

Routinely back up your data files to a network drive or diskette. If you lose your laptop and have not backed up your data, not only will you lose your hardware, but also your hard work and sensitive Company information.

## RESPONSIBILITIES

Users are required to secure their laptops in accordance with these standards.

## INFORMATION NON-DISCLOSURE AGREEMENTS

Information Non-Disclosure Agreements or Confidentiality Agreements are designed to contractually prevent proprietary information from being disseminated to unauthorized parties.

Datamation has three such contracts.

- “Employee” is for Datamation employees. Each employee should sign this confidentiality agreement prior to or on the date of hire. The agreement must be kept in the permanent employee file in Human Resources.
- “Contractor Employee” is for individuals who have been contracted through a contract/vendor company. The Datamation employee who is responsible for maintaining relations with this company should maintain this non-disclosure agreement. The agreement must be retained for 8 years after termination of the contract.
- Any company who has access to Datamation proprietary information signs the “Outside Vendors” non-disclosure agreement. A vendor employee on behalf of the company must sign it. This non-disclosure agreement is used when confidentiality agreement verbiage is not already included into the main vendor contract. The Datamation employee who is responsible for maintaining relations with this vendor should maintain this non-disclosure agreement. The agreement must be retained for 8 years after termination of the contract.

*INFORMATION NON-DISCLOSURE AGREEMENT*

(Employee)

Whereas, I have accepted employment from Datamation in a capacity in which I will have access to and be exposed to confidential and proprietary, technical, financial, and/or business information, and Datamation has agreed to employ me subject to its normal at will employment practices and the terms of this Information Non-Disclosure Agreement,

In consideration of my employment or continued employment by Datamation, I agree as follows:

1. The term "Information", as used in this agreement, includes but is not limited to specifications, drawings, sketches, models, samples, reports, plans, forecasts, current and or historical data, computer programs documentation and all other technical, financial, or business data.
2. "Proprietary Information" is defined as information which is in the possession or control of the Company, which is not generally available to the public in the form it exists at Datamation, and which the company desires to protect against unrestricted disclosure or competitive use. All information which I receive in connection with my employment at Datamation shall be regarded as Proprietary Information unless I am aware that it is generally available to the public in the form it exists at Datamation or that Datamation has intentionally made it available to the public.
3. I agree not to disclose, disseminate or release any Proprietary Information to anyone who is not an employee of Datamation unless I am specifically authorized to do so by Datamation- . Upon request, I will promptly return all Proprietary Information to Datamation.
4. In the event that I disclose, disseminate or release any Proprietary Information received from Datamation, in violation of this agreement, I am aware that I may then become subject to disciplinary action, including dismissal.
5. I understand that this Information Non-Disclosure Agreement will survive the termination of my employment at Datamation.

**SIGNED and AGREED to by \_\_\_\_\_ on \_\_\_\_\_.**

*INFORMATION NON-DISCLOSURE AGREEMENT*

(Contractor's Employee)

Whereas, in my capacity as an employee of \_\_\_\_\_, a supplier or goods and/or services to Datamation, I will have access to and be exposed to confidential and proprietary technical, financial and/or business information, and Datamation has agreed to allow me the access and exposure subject to the terms of this Information Non-Disclosure Agreement,

I agree as follows:

1. The term "Information", as used in this agreement, includes but is not limited to specifications, drawings, sketches, models, samples, reports, plans, forecasts, current and historical data, computer programs or documentation and all other technical, financial, or business data.
2. "Proprietary Information" is defined as information which is in the possession or control of the Company, which is not generally available to the public in the form it exists at Datamation, and which the company desires to protect against unrestricted disclosure or competitive use. All information which I receive in connection with my employment by Datamation shall be regarded as Proprietary Information unless I am told that it is generally available to the public in the form it exists at Datamation or that Datamation has intentionally made it available to the public.
3. I agree not to disclose, disseminate or release any Proprietary Information to anyone who is not an employee of Datamation unless I am specifically authorized to do so by Datamation. Upon request, I will promptly return all Proprietary Information to Datamation.
4. In the event that I disclose, disseminate or release any Proprietary Information received from Datamation, in violation of this agreement, I am aware that I may then become subject to legal action.
5. I understand that this Information Non-Disclosure Agreement will survive the termination of any services to Datamation.

**SIGNED and AGREED to by \_\_\_\_\_ on \_\_\_\_\_.**

*CONFIDENTIAL DISCLOSURE AGREEMENT*

(Outside Vendors)

In consideration of being asked to work with the \_\_\_\_\_  
(Division, Group, etc.) of Datamation Company (Datamation), including the opportunity to submit quotations and/or supply services/resources on the following Datamation project: \_\_\_\_\_ the undersigned agrees not to disclose to third parties, or other of the undersigned's personnel not directly associated with the project, any information given the undersigned by Datamation relating to such project or otherwise, nor to make any use of such information other than that authorized in writing by Datamation.

The provisions of the Agreement shall not apply to information:

- a) which was in the public domain or generally available to the trade prior to the undersigned's receipt thereof from Datamation or which subsequently becomes part of the public domain or generally available to the trade by publication or otherwise except by the undersigned's wrongful act; or
- b) which the undersigned can show as in the undersigned's possession prior to receipt thereof from Datamation or
- c) which was received by the undersigned from a third party having no obligation of secrecy with respect thereto.

All written and/or computer media formatted information given the undersigned by Datamation- shall be returned to \_\_\_\_\_ of Datamation- upon completion of the undersigned's obligations to Datamation under the aforesaid project.

[ COMPANY: \_\_\_\_\_ ]

BY: \_\_\_\_\_

TITLE: \_\_\_\_\_

DATE: \_\_\_\_\_

## Company Information Security Handbook

### Table of Context

<u>Section</u>	<u>Page</u>
Policy	
Information Security Policy and Standards	B-2
Standards	
User Accountability	B-6
Electronic Mail	B-8
Internet Access	B-10
Software Licensing and Use	B-12
Virus Protection	B-13
PC Laptop Security	B-14
Telecommunications	B-15
Information Classification	B-16

# Company Information Security Handbook

---

## Company Information Security Policy and Standards

### **PURPOSE**

This Policy and its related Standards state the requirements for protecting information resources at Datamation Company. The Policies and Standards have been developed to control business risks and ensure the proper Datamation image is presented.

### **SCOPE**

This Policy applies to all Datamation employees, contractors, vendors and/or suppliers, temporary staff members, and joint venture companies as well as any other person or company who accesses Datamation's network resources. All information, regardless of the media on which it is stored, as well as automated systems used to store, process, and transmit information, are included under this Policy. The Policy includes all computer-related activity while using Company equipment, on Company facilities, or when accessing Company information.

In addition, this Policy applies to information resources that have been entrusted to Datamation by an entity outside the Company.

### **POLICY**

Information is a valuable asset to the Company. The preservation of its integrity, confidentiality, and availability is essential to the success of Datamation. Measures must be taken to protect information and information processing systems against unauthorized use, modification, disclosure, and destruction, whether accidental or intentional. The method used to protect information resources must be consistent with the value of those resources.

### **ENFORCEMENT**

Management, Information Security, and Internal Audit Services have the right and responsibility to monitor the use of Company information resources and compliance with Information Security Policies and Standards. Specifically, management is responsible for enforcing Policies and Standards while Internal Audit Services is responsible for evaluating compliance with Policies and Standards.

### **COMPLIANCE**

#### **Laws of individual countries supersede the Information Security Policy and Standards.**

Any use of information resources other than to support Datamation's business objectives will be considered a violation of this Policy. Violations or suspected violations of Policy and related Standards must be reported immediately to the Information Security Department. Failure to comply with Policy and related Standards may result in disciplinary action up to and including termination of employment or contractual relationships. Datamation, at its discretion, may also pursue civil remedies or criminal prosecution.

### **RESPONSIBILITIES**

The protection of Company information is a basic responsibility of all employees and service providers.

#### *User Accountability*



# Company Information Security Handbook

---

Each user must have a unique user identification code and password to access Company computer systems. In addition, users are responsible and accountable for all actions performed under their user ID.

## *Electronic Mail*

Company E-mail systems are to be used for business purposes only. Datamation treats all E-mail messages sent, received, and/or stored in its systems as Company records. Company E-mail systems **must not** be used to continue, distribute, or circulate **chain letters** or **inappropriate/offensive content**.

Datamation does not assure any personal right of privacy for any E-mail message or document transmitted through the use of Company equipment or systems. Datamation reserves the right to access all E-mail messages transmitted through Company equipment or systems, without prior notice, and to disclose the message to any person or entity that Datamation deems appropriate. Datamation retains the right to determine the acceptable use of its E-mail systems.

## *Internet Access*

Authorized Internet users will behave in an ethical, legal and morally responsible fashion while representing the Company over the Internet.

## *Software Licensing and Use*

Only software developed or licensed to Datamation and approved by Information Technology Management may be installed on Company computing resources.

All employees are required to comply with software copyright laws and licensing agreements. **Unauthorized duplication of licensed software and documentation is strictly prohibited.**

All software developed by employees or contractors on behalf of Datamation is Company property and protected by copyright law from unauthorized use and duplication.

## *Virus Protection*

Company approved virus protection software must be installed, enabled and updated at least monthly to protect all Company computing assets from virus infection.

## *Access Controls*

Access control procedures must be established to protect data, software, and computing resources from loss, disclosure or misuse. Access to Company information and systems will be granted on a need-to-know basis based on job responsibilities.

## *PC Laptop Security*

Company owned computers systems, including laptops and desktops, must be secured at all times to prevent loss of the computer and the sensitive information contained within.

## *Information Identification and Classification*

Company information must be classified based on its sensitivity and value to the organization (i.e., the business impact if destroyed, damaged or disclosed). Classification of information will

# Company Information Security Handbook

---

be used to develop appropriate levels of access control. The current classifications of information and applications are as follows:

- **Private** – applies to information about employees, customers, suppliers or the company that could adversely affect the company, stockholders, business partners, and/or customers.
- **Critical** – applies to information where incorrect information or disruption in processing could result in significant monetary loss, embarrassment to the company, criminal or civil liability, significant productivity loss, or impairment of operations.
- **Financial** – applies to information which processes and records financial information such as company assets, liabilities, equities, operating results, pricing, budget, forecast, etc.

## ***Personal Data Protection***

All personal data of employees, customers, etc. must be obtained, processed, and protected in accordance with the standards outlined in this policy. In addition, employees must comply with any current or future privacy laws found in their resident countries.

All data systems remain the property of Datamation. There is no personal right of privacy maintained for any electronic equipment assigned to employees or the data stored on or created by that equipment. Datamation reserves the right to access and review any data retained or transmitted by its systems without prior notice, and disclose any information obtained to appropriate parties.

## ***Third Party Information Requests***

If Datamation information resources are placed in the custody of an outside entity, management will notify the outside entity of Policy and applicable Standards. Contracts shall specify the level of protection that the outside entity must provide for Datamation information resources while in the custody of the outside entity. Non-disclosure agreements and/or other applicable contracts must be established prior to providing access to company information.

## ***Incident Handling***

Users should report any unusual computer or network activity to the Information Security Department as well as the Security Department. The Information Security Department, along with other technical staff, will determine if an actual event has occurred, conduct an investigation at the request of Human Resources or Security, make appropriate notifications and mitigate the risk of the incident.

## ***Remote Access***

Remote access to all Datamation networks and resources may be permitted providing authorized users are authenticated, privileges are restricted, and data is encrypted across any public network (e.g., the Internet). This access must be approved in advance by the associate's manager or information owner. Such remote access is not a universal fringe benefit and may be revoked at any time for cause including unsatisfactory performance and non-compliance with security policies. Current remote access solutions consist of:

- Centralized Dial-up using strong authentication
- Dial-in and replication
- Virtual Private Network (VPN) with strong authentication, up-to-date virus protection and personal firewall (See Remote Access Policy & Acknowledgement Agreement for additional information)

# **Company Information Security Handbook**

---

## **EXCEPTIONS**

Requests for an exception to this Policy or its Standards must be submitted in writing to the Information Security Department. These requests must include the reasons for the exception or variance and planned alternative control measures. Requests for exceptions will be handled on a case-by-case basis.

## **REVISIONS**

The Policy and Standards will be revised as needed to reflect changes in the Information Technology environment and related business risks. Changes to the Policy and Standards require approval of Information Security and Senior Information Technology Management. Suggestions for revisions to the Policy and Standards should be forwarded to the Information Security.

# Company Information Security Handbook

---

## User Accountability

User IDs and passwords are a critical part of ensuring the confidentiality, integrity, and availability of information resources. All users are responsible for protecting their user IDs and will be held accountable for all actions performed with them.

### *User Accountability*

- Each user must be issued a unique user ID and password to ensure individual accountability.
- User IDs and passwords must be kept confidential.
- Sharing user IDs and passwords is prohibited except in extreme circumstances and only with written authorization from management.
- User IDs and passwords must not be posted or recorded where they can be viewed or accessed by others.
- Passwords must be changed immediately when reset by a security administrator, or if it is suspected that the password has been compromised (i.e., observed by a third party).
- Users must logout when leaving their PC unattended for any period of time or after 10 minutes of inactivity. User PC screen-savers with passwords should be activated.
- Users must turn off PCs or log off of all network resources at the end of the day.
- Passwords should be constructed so that they are not easy to guess, but avoid passwords that must be written down to be remembered.
- Do not allow others to look over your shoulder as you type your password. This is called shoulder surfing and can easily reveal your password.

### *Effective Passwords*

The following techniques can be used to create passwords that are not easily guessed but are still easy to remember.

- Mix upper and lowercase letters and numbers. For example: Gold24K, Go2Store and Cat7Dog.
- Make up acronyms. For example: NOTFSW (none of this fancy stuff works), APECSC (all programmers eat cookies and swiss cheese)
- Select a series of words with a common theme. For example: Candy bars - KITKAT and MARSBAR Cars – GRANDAM and MODEL T
- Use the phonetic spelling of a word(s). For example: LITEBULB, EZRIDR, and TELIFONE.

# Company Information Security Handbook

---

- Make up compound words. For example: AIRPLAIN, MALEMAN, and RAILRODE
- Replace certain letters for numbers in a typical word. Such as replace O with 0, I with 1, B with 8, S with 5, L with 7, or E with 3. For example: M0T0R5, ENG1NE, 8EAR1NG, and P1ST0N
- Use regular words but omit vowels or other common letters. For example: DWNHLL (Downhill), DATMTN (Datamation), XPLRNG (Exploring), and SCRTPLC (Security Policy)

## *Ineffective Passwords*

Easily guessed passwords must not be utilized as they increase the risk of unauthorized access to company computing resources and applications. To strengthen passwords:

- Do not use your name, initials, user ID, nicknames, family names, addresses, months, or seasons of the year.
- Do not use predictable patterns like: ascending or descending digits (1-2-3-4, 4-3-2-1), same character (55555), simple alphanumeric sets (W-X-Y-Z), using the abbreviation of a month along with the year (JAN98, DEC99), or keyboard sequences (qwerty, qawsed, asdfjkl).
- Do not use words associated with the Company such as DATAMATION, , CUSTOMER, SALES, GERMANY, or GENEVA.
- Do not use the following words as passwords: GUEST, SECRET, or PASSWORD.
- Do not use any of the above things spelled backwards, or in all capital letters.
- Do not use words that can be chosen from English or foreign dictionaries, spelling lists, or other word lists and abbreviations.
- Do not use other easily obtainable information. This includes pet names, license plate numbers, telephone numbers, identification numbers, the user's brand of automobile, and so on. Someone who knows the user could easily guess these passwords.
- Do not use a password of all numbers, or a password composed entirely of alphabet characters. Mix numbers and letters.

# Company Information Security Handbook

---

## Electronic Mail

The electronic mail (e-mail) systems provided by or used at Datamation are intended to assist employees and vendors in carrying out Company business by facilitating communication between individuals and work groups.

### *Management's Right to Access Information*

- E-mail messages are Company records. The content of e-mail, properly obtained for legitimate business purposes, may be disclosed within the Company without anyone's permission. Therefore, it should not be assumed that messages are confidential. Backup copies of e-mail messages may be maintained and referenced for business and legal reasons.
- The Company may inspect the contents of electronic messages in the course of an investigation, in the process of correcting a problem with a respective electronic mail tool, or at any time the Company deems necessary to inspect e-mail.

### *Message Content*

- The use of e-mail to transmit any message or file whose content violates any Datamation Policy or state or Datamation law is prohibited. Examples of prohibited use include, but are not limited to: Communications that contain defamatory, sexually-oriented, obscene, offensive, threatening, or harassing language or files that contain copyrighted materials for which required permission to use or distribute was not obtained.

### *Message Integrity and Disclosure*

- Incidental use of the e-mail systems to transmit messages of a personal nature will be treated by Datamation no differently than Datamation related business e-mail messages.

### *Safeguards of E-mail Systems*

- Employees are prohibited from the **unauthorized use** of passwords and encryption keys to gain access to other employee's e-mail messages. Only senior management can authorize such use.

### *Internet E-Mail*

- Unauthorized use of external mail services (examples: AOL mail, MSN mail, CompuServe mail) for company correspondence is expressly forbidden (authorization must be obtained from Information Security).
- Treat all information put into Internet electronic mail as if it were publicly available information. Internet electronic mail is susceptible to interception, redirection, or loss. As a result, electronic mail through the Internet must **not** be used as a secure method of communications for sensitive information.
- Treat all electronic mail correspondence as if it is a potential record that can be used in litigation. (Legal precedents exist where electronic mail has been subject to discovery in lawsuits.) Do not put information in Internet electronic mail correspondence that you would not put on Datamation letterhead paper correspondence.

# Company Information Security Handbook

---

E-mail must **NOT** used on the Internet to:

- Develop business processes that depend on guaranteed or reliable message delivery through the Internet unless the inherent unreliability of the Internet is accounted for in the process. Internet electronic mail is frequently delayed or lost and can **not** be counted on as a totally reliable message delivery system.
- Send or receive information with inappropriate humor or graphics. Use of electronic mail on the Internet must be in accordance with other Datamation policies.
- Distribute chain letters.
- Distribute personal opinions that do not reflect the stated position of Datamation.
- Distribute information that may be sensitive to Datamation.

## *User Responsibilities*

- Delete e-mail messages within a reasonable period of time. E-mail messages, attachments, and calendars utilize disk space that is shared among many other users and must be treated as a shared resource.
- Use e-mail consistent with its intended purpose. Do not use e-mail as a replacement for file transfer utilities. Attachments should be a business document of a reasonable size, not data files.
- Use e-mail consistent with its intended purpose. Do not use an e-mail account assigned to another individual to either send or receive messages. Use features/facilities such as message forwarding to allow others to read personal mail messages.

# Company Information Security Handbook

---

## Internet Access

The Internet provides a vast store of information and can be used to conduct business as well as research products, customers, competitors, legal concerns and other business issues. Due to the breadth of information stored on the Internet, precious employee time can be lost pursuing non-business issues or entertainment distractions.

Use of the Internet is for the support and improvement of Datamation business objectives. Access is a privilege, not a right, and individuals are responsible for their behavior and actions when accessing the Internet.

### *Acceptable Use*

While using Datamation Internet services you must **NOT**:

- Use Internet services for illegal purposes. If you are not sure of the legality of your actions, contact the Company Legal Department or Information Security.
- Use another person's name, password, security keys, files, and data or otherwise misrepresent your identity to other users or companies.
- Use computer programs or devices to circumvent, subvert or disable any security measures anywhere on the network.
- Intentionally engage in any activity that might be harmful to the computer or network systems or any of the information stored thereon. This includes, but is not limited to, creating or propagating viruses or worms, damaging files, or disrupting or denying services by intentionally overloading critical network systems.
- Use Datamation systems for commercial or political purposes not explicitly authorized by the appropriate Company management.
- Download any previously unlicensed software package for evaluation or business use. All software must be evaluated and approved via an Information Technology project.
- Use Company accounts or equipment to download entertainment software or games or play games over the Internet.
- Upload and/or download graphics, images or other material that is inappropriate or not in accordance with Company policies.
- Sell or distribute software through the Internet for personal commercial purposes.
- Post or upload sensitive Datamation information to any public Internet service where it can possibly be intercepted.
- Reveal the personal addresses or telephone numbers of employees or colleagues.



# Company Information Security Handbook

---

- Store, post, display, transmit, intentionally receive or exchange pirated software, stolen passwords, stolen credit card numbers, indecent or obscene material or other information inconsistent with Datamation business.

## *Public Representation*

- Datamation retains the copyright to any material created or electronically distributed by any authorized Internet user in the course of their duties. To avoid libel, distribution or transmission of negative comments or similar attacks on any person or entity, including Datamation competitors, is strictly prohibited.
- Authorized Internet users must never publicly disclose sensitive internal Datamation information, whether via electronic mail or other network services, including any information that may adversely affect Datamation's competitive position, customer/vendor relations or public image.

## *Infrastructure Monitoring*

- All use of the Internet services, including electronic mail, is subject to observation and monitoring by Company Information Technology, Information Security and/or Internal Audit to verify that the use of services is in accordance with Company policy. **There is no privacy or expectation of privacy in the use of any Company information systems or technologies.**

# Company Information Security Handbook

---

## Software Licensing and Use

The reproduction of copyrighted computer software without required authorization violates copyright laws in many countries, including the U.S. In the U.S., unauthorized software reproduction is a offense, and exposes both individuals and the Company to criminal penalties including fines and imprisonment. Software Vendors conduct compliance audits and can charge \$100,000 per violation.

### *Software Use*

- Purchase only approved standard hardware and software to ensure it is supportable and to minimize support time.
- All employees should be trained on software products prior to using them.

### *Software Licensing*

- All software installed on Datamation computers must be properly licensed such as with a Company site license, server-based license, individual workstation license, or negotiated contract.
- A sufficient number of copies of software must be purchased to ensure that it is used within the terms of the relevant licensing agreement.
- The reproduction of copyrighted software is prohibited unless authorized within the terms of the licensing agreement.
- Demo software obtained on a trial basis must be removed after evaluation unless properly licensed.
- Department specific software and files must be removed from microcomputers that are transferred to another department.

### *Appropriate Software*

- Personal software shall not be installed on Datamation- owned computers or equipment unless a business justification is documented and approved by location IT management.
- Games may not be stored or used on Datamation computers, except for those that are included with software licenses by Datamation.
- Public domain software, freeware, or shareware is not to be downloaded to Datamation computers from external networks, bulletin boards, or other sources.

## Virus Protection

The threat of computer virus attacks has increased dramatically in the last few years. The Virus Policy and associated Standards describe virus prevention techniques directed at minimizing the risk of virus infections to Datamation's information and computing systems.

- Anti-virus software shall be installed on all microcomputers (desktop and portable) and LAN servers connected to the WAN and stand-alone systems.
- Anti-virus software pattern files must be kept current. The pattern files must be updated every month. However, pattern files should be updated as they are available (i.e. weekly). These files require regular updating to protect against new viruses that appear regularly.
- All diskettes or CD's, regardless of where they come from, must be scanned for viruses before they are used. This includes demo software, shrink-wrapped software; diskettes/CD's used on home computers, as well as diskettes/CD's received from other Company departments.
- Files should be periodically backed up. It may be necessary to restore the system from backups after a virus infection.
- Employees who use their home computer for work-related purposes and whose department has licensed the virus scanning software for their file server must install virus software on their home computer.
- Report all new virus infections to the Information Security Help Desk at (011- 43038825) or the IT Help Desk.

## PC Laptop Security

The threat of stolen computers, especially laptops, has increased dramatically in the last few years. The Computer Security Policy and associated Standards describe prevention techniques directed at minimizing the loss of computers and the sensitive information contained within.

- Don't leave your laptop in an unsecured office or on a desktop when leaving for the day. Take the unit with you or secure it in a lockable office or lockable drawer out of sight.
- When going through airport security, wait until just before you step through the metal detector to place your computer on the belt for x-ray. Don't allow others to step in front of you. This is a scheme used by teams to pick up laptops.
- Never leave your laptop inside your vehicle when you go to a meeting. Place it in the trunk out of sight or take it with you.
- Keep your laptop with you in the lobby when you are checking into a hotel. Place the case on the floor between your legs, or step on the strap with your foot. Don't get distracted by strangers making conversation.
- Don't leave your laptop in your hotel room out in the open. Take it with you when you leave if possible, or conceal it inside your luggage bag, under the bed out of view, or at the front desk in a safe deposit box.
- Report the loss of any laptop immediately to Company Security and the local police. Keep a record of the unit serial number. This information can be quickly entered into the police database and improve the chances for the unit to be recovered in the future. This will also allow access to any Company networks to be quickly deleted.
- Routinely back up your data files to a network drive or diskette. If you lose your laptop and have not backed up your data, not only will you lose your hardware, but also your hard work and sensitive Company information.

# Company Information Security Handbook

---

## Telecommunications

Business communication is a substantial expense to Datamation each year, and failure to control these costs can effect the profits of the Company.

With the continuing increase in telephone fraud and misuse of company communication assets, there is need to manage telephone use and costs throughout the company. Telecommunication monitoring involves security over the telephone system, review of service provided by the carrier, and review of the costs associated with providing telephone service.

Employees should:

- Not dial 0# for any outside person requesting assistance.
- Not accept collect calls (except for emergencies).
- Not accept third party billing calls.
- Not transfer incoming calls to outside company numbers.
- Use good judgment when using company calling cards.
- Report all lost or stolen company calling cards immediately to Ms Sushma at 011-43038800

Management must:

- Understand and support the need for telephone system controls and recognize that cost control is a necessary part of Datamation's overall business objectives.
- Regularly (at least quarterly) review the billing analysis available from the service provider for improper traffic patterns and improper use.

# Company Information Security Handbook

---

## Information Classification

It is essential that adequate controls be provided to safeguard the integrity of data being processed through company computers. The possibility of direct financial loss, faulty management decisions or embarrassment to the company from disclosure of information must be minimized through the use of sound data protection methods.

Classifying information is the process of matching the assessed significance of the data to a level of access controls needed to protect it. It is the responsibility of the owner of an application to assess that need on behalf of the Company.

- All information must be classified by its owner into one of two classification levels: Sensitive or non-sensitive information. Sensitive information defined as Critical, Financial, or Private, must be protected from disclosure, modification, or destruction. Non-sensitive information or applications should conform to sound business practices.
- All information must have an identifiable owner. The owner, in most instances, will be the business unit primarily accountable for the business results achieved when using this information. They are responsible for the definition, use, and integrity of the data.
- Access to sensitive information and data files must be authorized by the owner of an application in accordance with its classification. This access approval must be documented in some verifiable form (e.g., signed memo, e-mail).
- Production information should retain the same level of security even if it is copied or moved from one computing platform to another (e.g., down-loaded from the mainframe to a personal computer).
- Datamation sensitive information must not be sent over the Internet, via electronic mail or by other means. Credit card numbers, telephone calling card numbers, internal log-in passwords and other parameters that can be used to gain access to Datamation's network, stand-alone computers, accounts, goods or services must not be sent over the Internet in readable form.
- Datamation software, documentation and all other types of internal information must not be sold or otherwise transferred to any non-Datamation party for any purposes other than business purposes expressly authorized by Company management. Sensitive information must not be transmitted to other Datamation employees who do not need to know this information.
- Information must be disposed of in a manner that protects against its disclosure or misuse.

All employees are responsible for information security and will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access.

# Internet Policy Acknowledgement

Form C

Anyone wishing to use the Company Internet facility must complete this form and have it signed by his or her respective manager, if appropriate.

- **All personnel must attend the in-house Internet Access at Datamation Overview or have waiver below signed.**
- I have reviewed a copy of Datamation's Internet policy and the Internet standards (Chapter 3: Internet Access in Datamation's Information Security Policy and Standards manual) and agree to comply with them.
- I realize that the company's security software may record for management's use the Internet address of any site that I visit, and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use.
- I know that any use of the Internet other than to support Datamation's business objectives will be considered a violation of this policy. Violations or suspected violations of this policy must be reported immediately to Information Security Department.
- **I know that any violation of this policy may lead to disciplinary action up to and including termination of employment or contractual relationships. Datamation, at its discretion, may also pursue civil remedies or criminal prosecution.**

\_\_\_\_\_  
Authorized Internet User's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Authorized Internet User's Printed Name

\_\_\_\_\_  
Location

- I have received a written copy of Datamation's Internet policy and the Internet standards (Section 3: Internet Access in Datamation's Information Security Policy and Standards manual) and fully understand them. The above Authorized Internet User, for whom I have budgetary responsibility, has a business need to access the Internet.

\_\_\_\_\_  
Manager's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Manager's Printed Name

\_\_\_\_\_  
Location

## FOR INTERNAL USE ONLY

Account ID

Date Completed/Notified

Created By

Date Deleted/Reason

# Remote Access Policy and Acknowledgement Agreement

Form D

---

## Datamation Remote Access Policy

### Rationale:

The objective of this policy is to ensure that all Datamation computer systems accessed by PCs using dial-up and “always on” (see explanation below) digital connections are appropriately protected. Technically adept (and often unscrupulous) individuals have relatively easy access to computers using always-on digital Internet connections. Undefended computers connected via digital connections to the Internet are believed to be in significant jeopardy of intrusion.

The Datamation servers to which these PCs connect are in turn put at risk. The accessibility of undefended home computers is generally well known within the “hacker” communities. The combination of broad knowledge and ever expanding usage of always-on digital connections requires Datamation to implement policies sufficient to protect our business assets.

“Always-on” digital connections include but are not limited to:

- xDSL
- Cable modem
- Satellite modem
- ISDN to Internet

### Policy:

Remote access to all Datamation networks and resources may be permitted providing authorized users are authenticated, privileges are restricted, and data is encrypted across any public network (e.g., the Internet). This access must be approved in advance by the associate's manager or information owner. Such remote access is not a universal fringe benefit and may be revoked at any time for cause including unsatisfactory performance and non-compliance with security policies. Current remote access solutions consist of:

- Centralized Dial-up using strong authentication
- Dial-in and replication
- Virtual Private Network (VPN) with strong authentication, up-to-date virus protection and personal firewall (See Remote Access Policy & Acknowledgement Agreement for additional information)

### Requirements:

Computers that access the Datamation network either through direct dial-up or Internet-based VPN (virtual private network) need to meet the minimum level of protection.

- Personal PCs that access the Internet and use the same PC to connect to the Datamation network are subject to this policy.
- This policy includes PCs on home networks that contain always-on connections.
- Personal PCs that **never** connect to the company network are not subject to this policy.
- PCs using VPN access **must** be firewall defened either through the use of a firewall software or hardware.
- Bypassing firewall security in any way is in direct violation of this policy.
- PCs subject to this policy **must** have current virus protection software installed and running.
- Laptops using a VPN (virtual private network) connection from any publicly accessible area can connect to the DM network if:
  - Laptops are not left unattended while connected to the Internet and /or DM network.
  - Virus and firewall software (if required above) is loaded and current.



# Remote Access Policy and Acknowledgement Agreement

Form D

## Standards:

- I know that any use of any remote access connection to Datamation other than to support Datamation's business objectives will be considered a violation of this policy. Violations or suspected violations of this policy must be reported immediately to the Information Security Department.
- I will install, at my own expense, McAfee Anti-Virus software, or equivalent commercially available virus software packages, which must be running on the remote client PC at all times. Anti-virus software for Datamation PCs will be installed at the company's expense. At least on a monthly basis, the most recent software updates, including DAT files, **must** be installed. If I am connecting to the DM network using a non-Datamation PC, then it is my responsibility to pay for the necessary virus protection software. I will provide "proof" of virus protection to IT management upon request.
- For VPN remote access, I will install, at my own expense, personal firewall hardware or software to protect the PC which the VPN client software will be installed. Firewall software for Datamation PCs will be installed at the company's expense. Firewall hardware consists of a Netgear, D-link or Linksys router. Recommended firewall software includes McAfee Firewall or Norton Personal Firewall. This software must be running every time I connect to the Internet and/or the VPN to Datamation's network. The software configuration must also be set at a minimum Security Level of Nervous. If I connect to the Internet via a permanent connection, such as cable modem or DSL, I will ensure the firewall equipment is running each time I connect to the Internet. I will provide "proof" of firewall protection to IT management upon request.
- If I purchase any hardware or software to support remote access to Datamation, I personally own this equipment and am responsible to be in compliance with the licensing agreement of such equipment.
- If I plan connecting via DSL or Cable access, I realize that all Cable and DSL providers have rules that may restrict the use of VPN services across their network. I will abide by those rules and regulations.
- I realize that the company's security software may record, for management's use, the remote network activity in which I engage. I acknowledge that any message I send or receive may be recorded and stored in an archive file for management use.
- I will comply with all Information Security Standards as seen on the Datamation Information Security web site especially related to the securing of passwords as to not allow others in the remote work location to gain access to passwords for Datamation business systems. I will also secure inactive PC sessions to restrict people in the remote work location from gaining access to the Datamation network. The security standards are located at in the Information Security Manual (ISM) in chapter 1.
- If I plan on using a non-Datamation PC to establish a remote connection:

# Remote Access Policy and Acknowledgement Agreement

Form D

- 
- I am responsible for ensuring compliance with all license agreements for all software loaded on the non-Datamation PC, except for the software provided by Datamation- . I acknowledge that Datamation is not responsible for managing software licensing on any non-Datamation PC.
  - I understand that Datamation is not responsible for repercussions of installing any client software on a non-Datamation PC.
  - The Release Notes for any client software must be reviewed to ensure compatibility with existing software.
  - A complete backup of the PC must be done to ensure recoverability of my data if the client software causes problems with existing software. If backup of the entire PC is not possible, I will backup the data and ensure original install disk/CDs are available for possible reinstallation.
  - DATAMATION COMPANY IT can provide consultation for firewall implementation at the “courtesy” level.
  - Visits for assistance to private residence(s) are not available.
  - “Bring it in, we’ll look at it” support is not available.
- Upon termination of my employment or contract with Datamation, any software provided by Datamation will be uninstalled from the non-Datamation PC. This includes the VPN client, firewall, and virus software.
  - **I know that any violation of this policy may lead to disciplinary action up to and including termination of employment or contractual relationships. Datamation, at its discretion, may also pursue civil remedies or criminal prosecution.**

# Remote Access Policy and Acknowledgement Agreement

Form D

## Remote Access Acknowledgement Agreement

### Remote Access User Signoff

Anyone wishing to use the Company RAS (Remote Access Server) or VPN (Virtual Private Network) connection must complete this form and agree to the terms of the Remote Access Policy. They must sign this acknowledgement to indicate their agreement to these terms and have their manager's approval below.

I know that any violation of the Remote Access Policy or the Information Security Policy may lead to disciplinary action up to and including termination of employment or contractual relationships. Datamation, at its discretion, may also pursue civil remedies or criminal prosecution.

Do I already have a SecurId card? SecurId authentication is required. YES / NO (Circle One)

Authorized User's Signature

Date

Authorized User's Printed Name

Location

### DM Manager Signoff

- I request the above user have access to the Datamation network via the RAS or VPN connection.
- I acknowledge that the above User has agreed to comply with the Remote Access Policy.
- I am responsible for the costs associated with the following software, if needed, by the above user:
  1. Firewall Software, comes with FiberLink package supplied to all DM laptops (No charge) (Hardware firewall costs are responsibility of User not DM)
  2. Ethernet PC card, if user's laptop does not already have one (Needed only for Cable or DSL access. Ordered and Paid by User department)

DM Manager's Signature

Date

DM Manager's Printed Name

Location

Please return this Acknowledgement Signoff Sheet (this page only) to the Information Security department in New Delhi, at fax 011-22240086.

Please contact the helpdesk for assistance with this questionnaire at 011-43038825.

For Security/HelpDesk Use Only	When complete, Initial and Date below	
Reviewed and approved the Acknowledgement Form?		
Fiberlink User Created? (if necessary)	UID=	PW=
SecurId ACE Server VPN Access completed?		

# Security Awareness Policy Acknowledgement

Form E

Any one wishing to use any Information within the Datamation Company facility must complete and sign this form.

- **I have attended the Security Awareness Training Presentation, or viewed the Security Awareness Video, and received a written copy of the Datamation Company Information Security Handbook.**
- I have reviewed a copy of Datamation’s Company Information Security Handbook (Section/Form: B Datamation) and agree to comply with the Information Security Policy and Standards.
- I realize that the company’s security software may record, for management’s use, the type of access that is being used by my personal userid and password.
- I know that any use of my userid and password, other than to support Datamation’s business objectives will be considered a violation of this policy. Violations or suspected violations of this policy must be reported immediately to Company Information Security Department.
- **I know that any violation of this policy may lead to disciplinary action up to and including termination of employment or contractual relationships. Datamation, at its discretion, may also pursue civil remedies or criminal prosecution.**

\_\_\_\_\_  
User’s Signature

\_\_\_\_\_  
Date

User’s Printed Name

Location