STI GROUP DISCUSSION WRITTEN PROJECT

eDISCOVERY FOR GIAC ENTERPRISES - DATA CLASSIFICATION, RETENTION, AND LITIGATION POLICIES AND PROCEDURES

Version 1.1

September 22, 2007

Team: Russell Meyer, Brad Ruppert

Developed for

www.sans.edu

Contents

1 Introduction

1.1 Overview

This presentation will define the policies and procedures surrounding eDiscovery for GIAC Enterprises which is the largest supplier of Fortune Cookie sayings in the world. Policies and procedures around data labeling, classification, data retention, and litigation will be discussed in detail. The implementation details and architecture of eDiscovery will also be discussed specific to GIAC Enterprises.

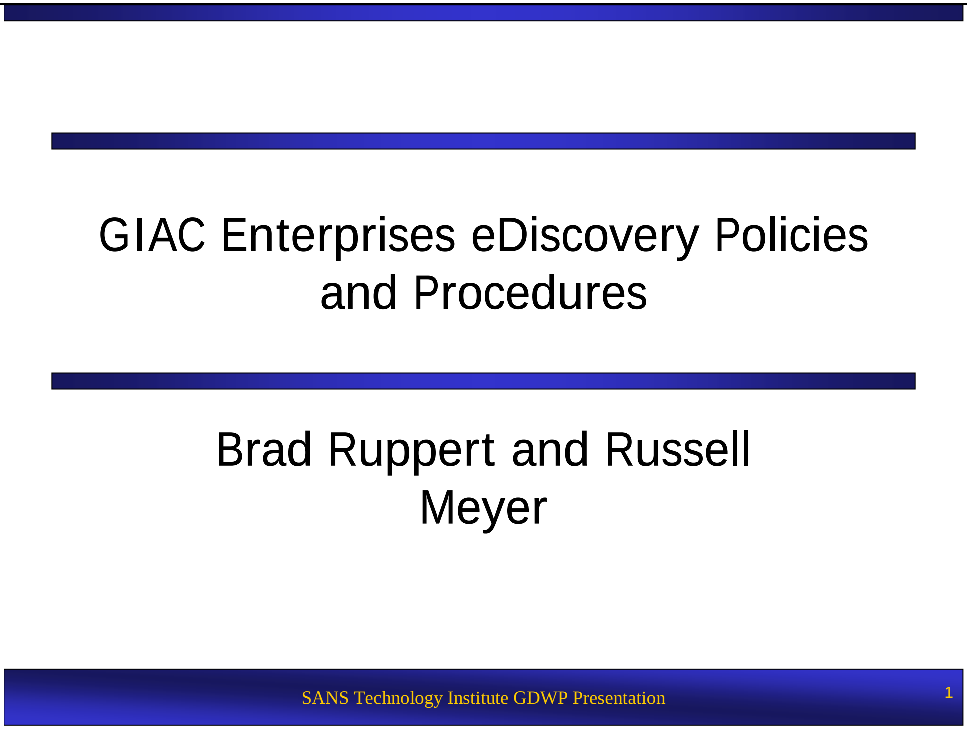
1.2 What is eDiscovery

Electronic discovery, or "e-discovery", refers to discovery of information in electronic form with regard to in civil litigation. This includes information stored on computers of an intangible form, volume, transience, and persistence which is different than paper. Additional components associated to electronic information are the attributes or metadata. This includes references to who created the data, who modified it, when it was created, its file size, etc. This presents new challenges and opportunities for attorneys and their clients, as well as the courts, as electronic information is collected and reviewed.

1.3 History of eDiscovery

“Electronic discovery (e-discovery) is a topic traditionally limited to legal circles. Recent case law and the December 2006 revision to the Federal Rules of Civil Procedure (FRCP) are aimed squarely at judges and lawyers. However, both changes have profound implications for information technology (IT) organizations, given the significant amount of electronically stored information (ESI) that is relevant for court cases. In essence, IT teams are strategic helpers for enterprise litigation, and the choices they make for the creation, storage, archival, and destruction of information have big impacts on legal and regulatory evidence handling. Because the information lifecycle involves data availability, confidentiality, and integrity, e-discovery is an important issue for enterprise security teams.”[1]

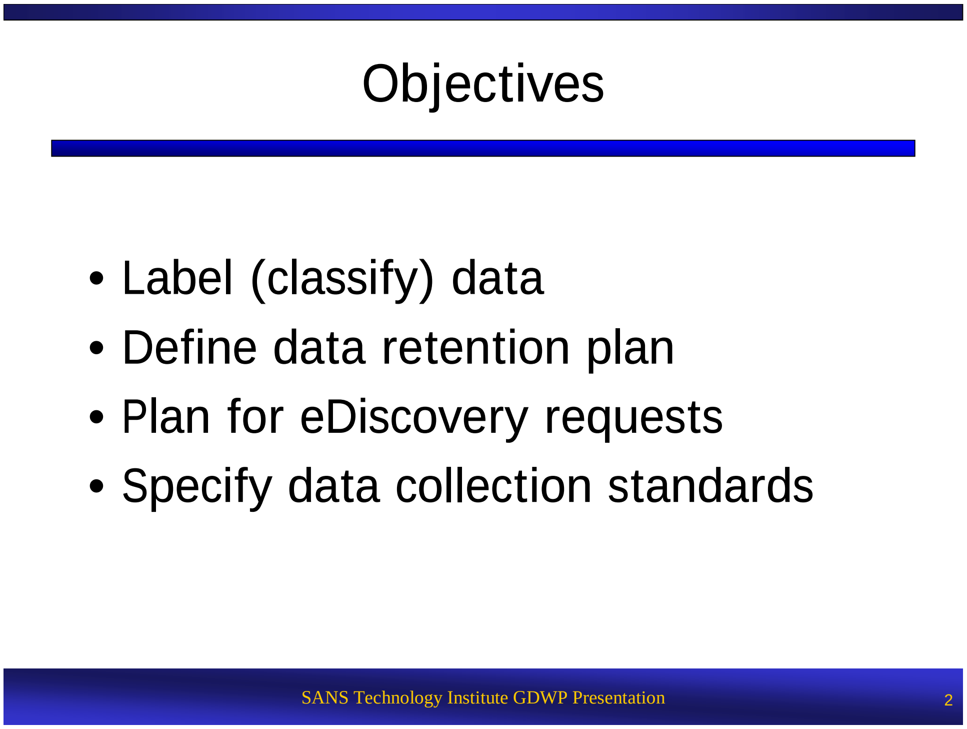
[1] Trent Henry, E-Discovery: No More Losing Needles in the Electronic Haystack, Burton Group. Mar 2007



GIAC Enterprises eDiscovery Policies and Procedures

Brad Ruppert and Russell Meyer

SANS Technology Institute GDWP Presentation 1



Objectives

- Label (classify) data
- Define data retention plan
- Plan for eDiscovery requests
- Specify data collection standards

SANS Technology Institute GDWP Presentation 2

2 GIAC Enterprises Data Labeling Policy

2.1 Purpose

The purpose of this data labeling policy is to provide a framework for protecting GIAC Enterprises information resources. Information resources are assets of GIAC Enterprises and must be classified by the sensitivity and associated risks to confidentiality, availability, and integrity. Data with the highest sensitivity and risk need the greatest amount of protection. Consistent use of this classification system will facilitate business activities that apply appropriate levels of protection.

2.2 Scope

This policy is applicable to all company assets created or maintained by GIAC Enterprises.

2.3 Background

All GIAC Enterprises information must have a primary responsible person, henceforth referred to as the Information Steward. It is each individual's responsibility to apply and comply with this Standard whether as a user, steward, custodian or recipient.

The Information Stewardship Standard describes two primary sources of GIAC Enterprises Information:

- Information materials created by a GIAC Enterprises employees or contractors
- Information maintained by GIAC Enterprises

Information Materials

In daily business operations, employees or contractors create/oversee a great deal of valuable information materials. The creator of information is responsible for:

- Determining use of materials
- Information classification/labeling
- Reclassifying the information when value/risk has changed
- Disclosure of information

The creator of information is by default the Information Steward, unless otherwise delegated.

Information Maintained by GIAC Enterprises

The Information Steward is responsible for:

- Adhering contract terms with the data provider /controller
- Ensuring contingency plan exists or is created
- Access authorization on a need-to-know basis

- Decisions regarding the permissible uses of information including relevant business rules
- Implementing sufficient controls to ensure data integrity
- Application of relevant controls for information consistent with policies and standards
- Documenting the names of the Information Stewards of any Technical Proprietary information

2.3.2 Information Custodians

Information Custodians are individuals who have physical or logical possession of information contained in corporate data systems. Information Custodians are responsible for protecting the information in their possession from unauthorized disclosure, alteration, or destruction and maintaining the integrity and availability of the information through the use of appropriate access controls as defined by the Information Steward.

2.3.3 Information Users

Information Users are individuals who have authorization to access, modify, delete information in the performance of their job function. Information Users must:

- Use the information only for legitimate business purposes
- Comply with all security measures defined by the security policy
- Refrain from disclosing business sensitive information
- Report any incident of a security vulnerability or violation to Information Security

2.3.4 Designating Information Stewards

Information Stewards for GIAC Enterprises data systems are the senior business unit managers of the system. If there are several potential Information Stewards, executive management must assign Information Stewardship responsibility to the manager of the business unit who makes the greatest use of the information.

2.3.5 Designating Information Custodians

Information Stewards of GIAC Enterprises data systems are responsible for assigning the role of Information Custodian. Although special care must be taken to clearly specify security-related roles and responsibilities when external parties are involved, it is permissible for Information Custodians to be contractors, consultants, or temporary staff.

2.3.6 Designating Information Users

Information Users may be employees, or any GIAC Enterprises contractor with whom special arrangements (such as non-disclosure agreements) have been made. All Information Users must be authorized by the Information Steward or their designate.

2.3.7 Contractor provided Information

Whenever information is received from a contractor, an Information Custodian shall be assigned. This individual shall be responsible for safeguarding information based upon the contractor's handling instructions and/or industry standards/contractual terms. GIAC Enterprises shall conduct a risk assessment to evaluate the protection of information should a contract not exist.

2.3.8 Risk Assessment Process

A security risk assessment process shall be established to address the importance of information to facilitate the classification process. The importance is comprised of three components – Confidentiality, Integrity and Availability.

All business units shall complete a business and risk impact analysis to ensure confidentiality, integrity and availability of their systems.

2.3.9 Business and Risk Impact Analysis

The importance of all GIAC Enterprises information assets shall be evaluated by determining the loss impact (in terms of the potential for brand degradation and adverse impact to management decisions, system operations, business functions, etc.) of such information assets, in order to ensure that the cost to protect each asset is appropriate for the overall level of risk.

2.3.10 Vulnerabilities and Threats

Circumstances that can increase the likelihood of unauthorized disclosure, alteration, or destruction of GIAC Enterprises information assets shall be identified as threats or vulnerabilities. These shall be recorded in terms of adherence or non-adherence with GIAC Enterprises security standards or policies. Mitigating controls shall be created to protect the systems based on the identified threats and vulnerabilities.

2.3.11 Mitigation of Risk

A plan to mitigate risks associated to the confidentiality, integrity and availability of GIAC Enterprises assets shall be developed. Mitigating controls shall be chosen based on the projected business impact analysis of a loss or breach. Business units shall perform risk assessments during the development phases of projects or if the system is significantly modified.

2.3.12 Data Classification

Upon completion of the security risk assessment GIAC Enterprises information assets shall be classified as one of the following five classifications:

- *GIAC Enterprises Public* – Information that has been explicitly approved by GIAC Enterprises management for release to the public.
- *GIAC Enterprises HIPPA*– All GIAC Enterprises employee health related records, history, and insurance information.
- *GIAC Enterprises HR*– All GIAC Enterprises employee related policies, benefits, wages, and personal information.
- *GIAC Enterprises Business Proprietary*– All GIAC Enterprises non-public information that cannot be clearly classified as Confidential or Restricted.
- *GIAC Enterprises Technical Proprietary* – The most highly sensitive or critical information that is restricted among GIAC Enterprises employees, GIAC Enterprises legal entities or business units specified by the Information Steward that would affect the competitive position or have a substantial detrimental impact if it were released.

2.3.13 Control Lifecycle

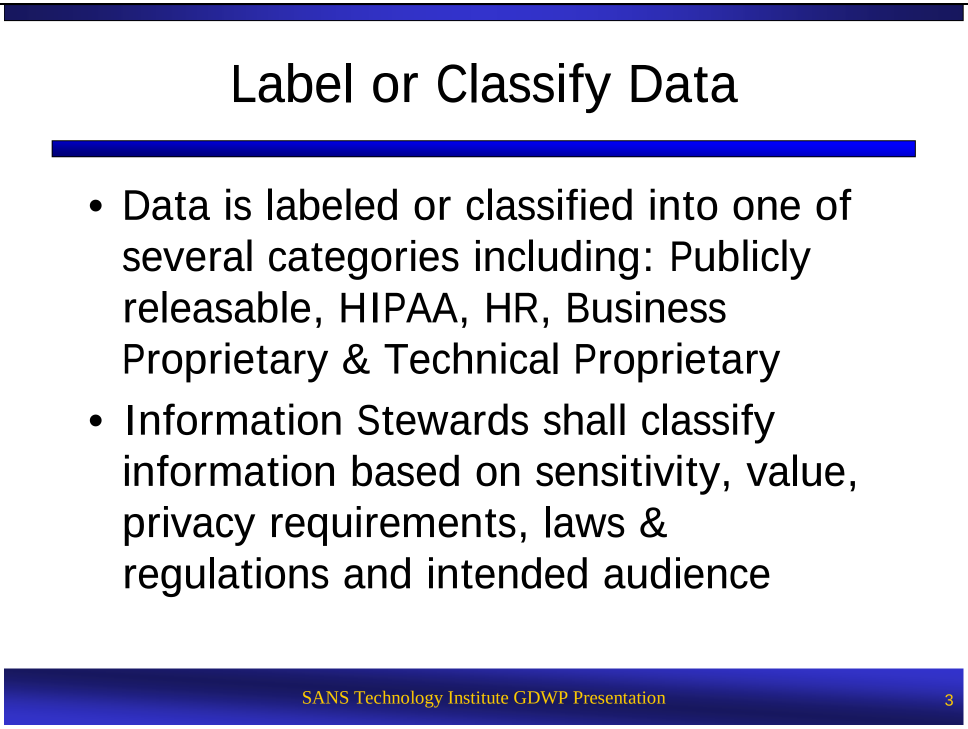
Information Custodians and business units share responsibility with the Information Stewards for protecting the information assets and shall implement, at a minimum, the following controls according to the documented sensitivity and criticality classification:

Classification of Information

Information Stewards shall classify information based on sensitivity, value, privacy requirements, laws and regulations and intended audience into one of the following five levels: Public, HIPAA, HR, Business Proprietary, and Technical Proprietary as described above. To help reduce the business impact of information restrictions and costs, the steward must assign the lowest level of classification required.

Classification Modification/Review

The designated Information Steward may determine that information requires reclassification, due to an incorrect initial classification, the effects of time sensitivity, a change in the nature of the information, or a change in the classification policy that warrants change. Notification must be sent to the custodians and users after a change is made to an asset's classification. Only after approval from an Information Steward may users move information to a less sensitive level.



Label or Classify Data

- Data is labeled or classified into one of several categories including: Publicly releasable, HIPAA, HR, Business Proprietary & Technical Proprietary
- Information Stewards shall classify information based on sensitivity, value, privacy requirements, laws & regulations and intended audience

3 GIAC Enterprises Data Labeling Procedure

3.1 Purpose

The purpose of GIAC Enterprises Data Labeling Procedure is to provide a means for all employees to appropriately classify and label information assets to help protect confidentiality, integrity, and availability of information assets. This protection reduces GIAC Enterprises' exposure from abuse and misuse of the information while increasing the security of the information by applying the appropriate security controls.

3.2 Procedure

3.2.1 Information Labeling

Information shall be classified from creation date until destruction and shall be labeled with the appropriate information classification designation including the "GIAC Enterprises" prefix. Information without a label is by default, classified as Business Proprietary. All other information must be labeled as defined in the GIAC Enterprises Labeling Policy.

All contractor or externally provided information, which is not clearly in the public domain, shall receive a GIAC Enterprises information classification system label, excluding copyrighted software. The GIAC Enterprises employee who receives this information shall be responsible for assigning an appropriate classification on behalf of the third party. This employee must preserve copyright notices, author credits, guidelines for interpretation, as well as information about restricted dissemination.

3.2.2 Internal and External Mail

If Technical Proprietary information is to be sent through external mail, or by courier, it must be enclosed in two envelopes or containers (double wrapped). The outside envelope or package must not indicate the classification or the nature of the information contained therein. The inside sealed and opaque package must be labeled with the appropriate classification. Packages containing business sensitive information must always be addressed to a specific person or to a designated content receiving point including return address information.

Confidential information that is sent through GIAC Enterprises internal mail must be placed in a sealed envelope and marked accordingly. Business sensitive information must never be sent via internal mail.

3.2.3 Printing or Faxing Sensitive Information

Unattended printing or faxing of business sensitive information is permitted only if physical access controls are used to prevent unauthorized persons from viewing the materials.

3.2.4 Classifying GIAC Enterprises information assets

1. The Information Steward categorizes the data into the appropriate classification via risk assessment. There are (3) levels of risk assessments:
    - S**imple** (single item review or the information asset has a relative medium corporate value)
    - **Medium** (multi-item or the information asset has relative high corporate value)
    - **Comprehensive** (a detailed assessment assessing crucial GIAC Enterprises information assets)
2. The following items need to be taken into consideration when classifying information prior to and after completing a risk assessment:
    - Information confidentiality considerations (trade secrets, fortune cookie sayings)
    - The business value of the information (financial, intellectual, marketing value, etc.)
    - Regulatory or legal considerations
    - Who will require access the information (information usage and their roles)
3. It is strongly recommended that a risk management professional perform the risk assessment process.
4. Upon completion of the risk assessment process, GIAC Enterprises data is to be categorized and labeled into one of the following five classifications:

GIAC Enterprises Public	**GIAC Enterprises HIPAA**	**GIAC Enterprises HR**	**GIAC Enterprises Business Proprietary**	**GIAC Enterprises Technical Proprietary**
Information explicitly approved for release to the public	Disclosure infringes upon legal and regulatory compliance violations.	Sensitive employee benefits, work history, wages.	Information not classified as confidential or restricted.	Highest level of sensitivity. Accountability is required.

5. After the GIAC Enterprises data is classified, the Information Steward follows the labeling and handling directives
6. Questions regarding classification are to be submitted to your immediate manager.

3.2.5 Classifying “non-category” data

1. If the Information Steward cannot classify the data, he/she can request the help of the immediate manager, or information security. This should result in one of the following cases:
    - The data is properly classified
    - A deeper level of risk assessment is required
    - Inclusion of additional classification or exceptions to policy

- Escalation to the executive management for additional help

3.2.6 Changing previously classified data

1. If there is a significant change to the data, a new risk assessment should be completed.
2. To determine the new classification of the data, the steward has the option of:
    - Assessing only the portion of the data that has been modified
    - Completing a new risk assessment reviewing all aspects of the data asset, the impact of the new change to the asset and who the new users of the data will be
3. If the new classification will require an increase in security controls, the Information Steward must cease current access to the data asset until the appropriate classification and associated security controls can be implemented.
4. Any changes to an asset's classification must be communicated to any relevant users of the data

Questions regarding classification changes are to be submitted to your immediate manager.

3.2.7 Classification of Metadata Attributes

The following represents a list of attributes that should be maintained for proper asset classification:

- Creation_date
- Version
- Last_modification_date
- Owner
- Personally_identifiable
- Data_subject
- Sensitivity (public, HIPPA, HR, business proprietary, etc.)
- Source (project, person, or application contributing the information)
- Purpose (business purpose of information)
- Type
- Attribute_authority (who or what applied these attributes to this item)

4 Data Retention Policy

4.1 Purpose

The purpose of this policy is to provide guidance regarding data retention which includes backup requirements, protection, storage, data categories, and enforcement.

4.2 Scope

This policy applies to all GIAC Enterprises employees, contractors and affiliates.

4.3 Policy

4.3.1 Backup and Retention

Information and System Equipment Stewards shall ensure GIAC Enterprises information assets are backed up regularly for operational recovery purposes as well as to comply with Business Continuity Recovery Plans and that backups are retained in accordance with business unit retention requirements.

4.3.2 Backup Requirements

All data that has ongoing business value, regardless of data classification or location, shall be backed up. As required to preserve business systems recoverability, the System Equipment Stewards shall perform both differential and full backups of their information and shall verify the integrity of the backup upon its completion.

4.3.3 Protection

The media used for backups shall be regularly tested for reliability and integrity. The information restoration procedures shall be regularly tested for effectiveness and acceptable performance.

4.3.4 Storage

Where required, GIAC Enterprises Staff shall be provided facilities to create and store backups of information. Any backup media stored onsite shall be stored in a physically and environmentally secured area based on the handling requirements applicable to the asset's classification. The Equipment Steward shall ensure that offsite storage has adequate environmental and physical controls to protect media. A list of personnel authorized to remove backups from the offsite location shall be maintained at all times.

4.3.5 Retention

All information including backups, email, documents, consumer data, customer data and third party information shall be retained based on the requirements of the Information Steward and any applicable statutory and/or regulatory requirements. The Legal Department may direct the suspension of routine data destruction schedules so that GIAC Enterprises may comply with a court order.

4.3.6 Data categories

Publicly releasable data

Data generated by the company for public release will be kept a minimum of five (5) years from date of public release or as required by law. The information may be kept longer depending on it historical value and storage expense. Data protection for publicly releasable information should focused availability and integrity of rather then access restriction. Data backups should follow regular backup procedures for non-sensitive information. When publicly releasable data is disposed of, the appropriate data destruction guidelines for non-sensitive information should be followed.

HIPAA data

Data that falls under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 shall be kept six (6) years as defined by the HIPAA Privacy Rule or longer as required by state or other regulations. Data protection for HIPAA related information should include security (access restriction) as well as data availability and integrity. Data backups should follow regular backup procedures for sensitive information. When publicly releasable data is disposed of, the appropriate data destruction guidelines for sensitive information should be followed.

HR data

HR (Management to Employee) data will be kept for the duration of the employee’s tenure and then two years after termination of employment date or longer as required by state or other regulations. Data protection for HR data should include security (access restriction) as well as data availability and integrity. Data backups should follow regular backup procedures for sensitive information. When HR data is disposed of, the appropriate data destruction guidelines for sensitive information should be followed.

Business Proprietary

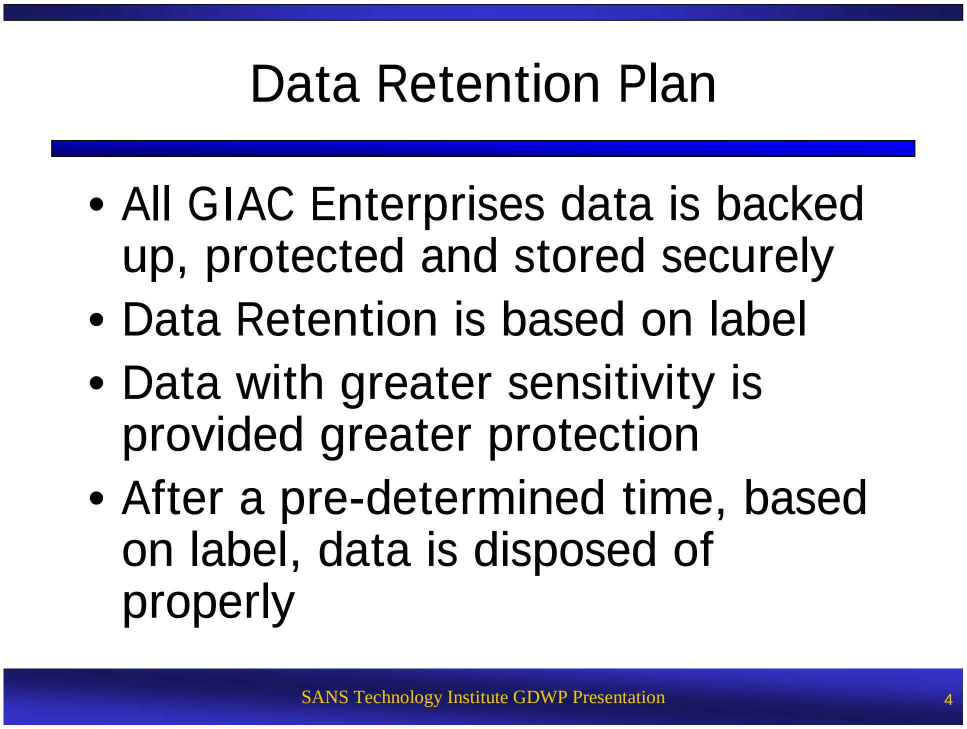
Business Proprietary (Contact lists, contracts) data will be kept for five (5) years or longer as required by state or other regulations. Data protection for Business Proprietary data should include security (access restriction) as well as data availability and integrity. Data backups should follow regular backup procedures for sensitive information. When Business Proprietary data is disposed of, the appropriate data destruction guidelines for sensitive information should be followed.

Technical Proprietary

Technical Proprietary (know how, trade secrets, technical advantage, list of things known not to work) data will be kept indefinitely. Data protection for Technical Proprietary data should include security (access restriction) as well as data availability and integrity. Data backups should follow regular backup procedures for sensitive information. Archiving of Technical Proprietary data should be considered due to costs of online or onsite storage.

4.3.7 Enforcement

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



Data Retention Plan

- All GIAC Enterprises data is backed up, protected and stored securely
- Data Retention is based on label
- Data with greater sensitivity is provided greater protection
- After a pre-determined time, based on label, data is disposed of properly

SANS Technology Institute GDWP Presentation 4

5 GIAC Enterprises Litigation Procedure

5.1 Purpose

The purpose of this procedure is to provide guidance regarding data retention, discovery and recovery during litigation.

5.2 Scope

This policy applies to all GIAC Enterprises employees, contractors and affiliates.

5.3 Procedure

The steps listed below should be the followed once the Legal Department is notified of the discovery request:

5.3.1 A data destruction hold is issued

The Legal Department quickly reviews the discovery request and working with the appropriate Information Stewards (business owners), Information Custodians (IT system administrators, DBA, etc.) immediately requests a “data destruction hold” on the data in question. This “data destruction hold” should cover all data that may fall under the discovery request. This includes any actions needed to save or prevent the normal destructions of data. For example, metadata or log file data is not normally saved or backed up should be saved or backed up to prevent its loss. At this point, it is better to save too much data. Live or transactional data should be considered as well. Document the chain-of-custody when handling and securing data.

5.3.2 Discovery review

The Legal Department reviews the discovery request and working with the appropriate Information Stewards and Information Custodians and determines exactly which information is covered by the discovery request. This step may identify additional information that needs to be added to the “data destruction hold” list as well as identify data that is under the data destruction hold that no longer needs to be protected.

5.3.3 Data Retrieval

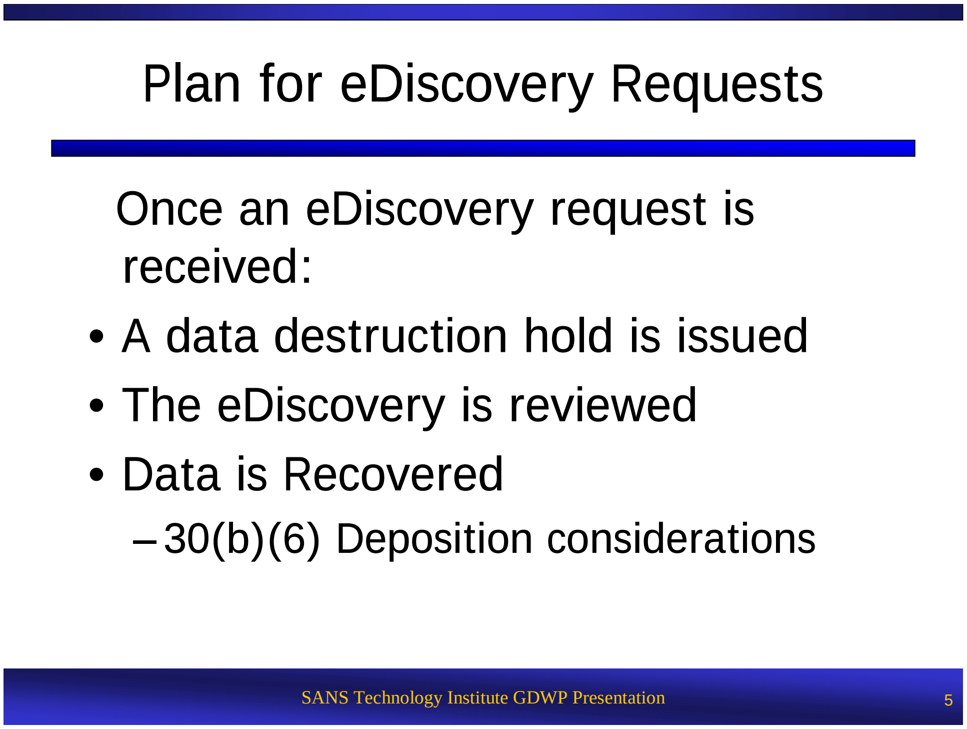
Once the data subject to discovery has been determined, the Legal Department in concert with the appropriate Information Stewards and Information Custodians determines the best way to retrieve the data. This could include special data forensic tools for data extraction. The format of the data delivery is determined. The amount of time required to extract the data is discussed, estimated and approved. If more resources are needed to meet deadlines, management is informed. Chain-of-custody is documented and the data recovered is kept secure. An appropriate delivery method, for example registered mail, is determined. A copy of data provided should be kept (if not cost prohibitive) until legal determines it is no longer needed.

5.3.4 30(b)(6) Depositions

If there is a possibility of a 30(b)(6) deposition, the data recovery process should be documented in such a way that an employee with IT knowledge could understand the recovery process. The Legal Department will determine if there is a possibility of a 30(b)(6) deposition requirement and who will be designated to speak for the company at the deposition.

5.3.5 Hardware, Software and Media

In order to ensure the integrity of the data, the use of personal hardware, software or media during the discovery process is prohibited. Media used for the discovery process should be new and property of GIAC Enterprises. All software used should be licensed by GIAC Enterprises; free or open source software is discouraged. Any personal hardware, software or media used must be documented.



Plan for eDiscovery Requests

Once an eDiscovery request is received:

- A data destruction hold is issued
- The eDiscovery is reviewed
- Data is Recovered
  - 30(b)(6) Deposition considerations

SANS Technology Institute GDWP Presentation 5

6 Data Collection or Discovery Standard

6.1 Purpose

The purpose of this standard is to outline the acceptable locations for data storage in order to ease backup and data discovery in the case of litigation.

6.2 Scope

This policy applies to all GIAC Enterprises employees, contractors and affiliates.

6.3 Data collection or discovery standard

GIAC Enterprises data needs to be kept secure in order to operate efficiently. In order to keep the data secure, the locations of the data must be known to GIAC Enterprises. This will allow GIAC Enterprises to backup the data as well as assist in any discovery requests.

The following physical locations are approved for data storage

- Main data center
- Remote data center (co-location facility)

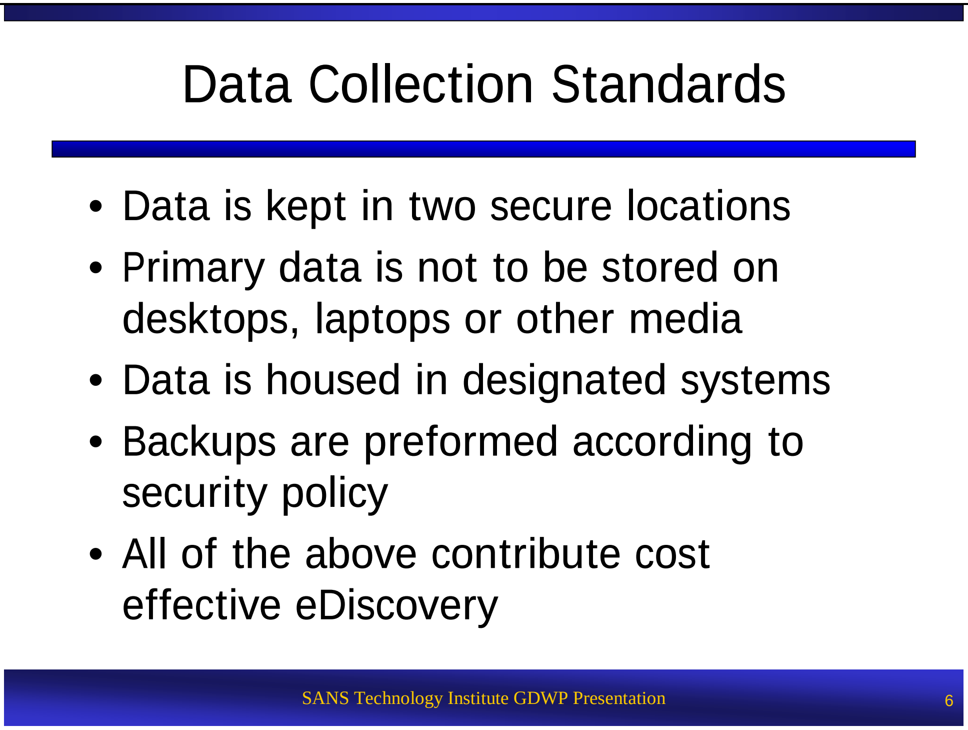
Data storage outside of the locations listed above is prohibited. For example: the corporate office, home-office or on portable media, including but not limited to:

- Laptops
- PDAs
- USB ‘thumb’ drives
- External hard drives
- Backup tapes
- CD or DVDs
- Internet based storage

Primary Email storage (for example, PST files) on desktops, laptops or PDA is prohibited.

Any server or device at a locations listed above that contains GIAC Enterprise data (including but not limited to: files, folders, databases, log files, transactional files, email, configuration files, voice mail, facsimiles) must be backed up via the centralized backup tape system. Any system or device that cannot be backed up by the centralized backup tape system should be backed up by another means and documented for accountability.

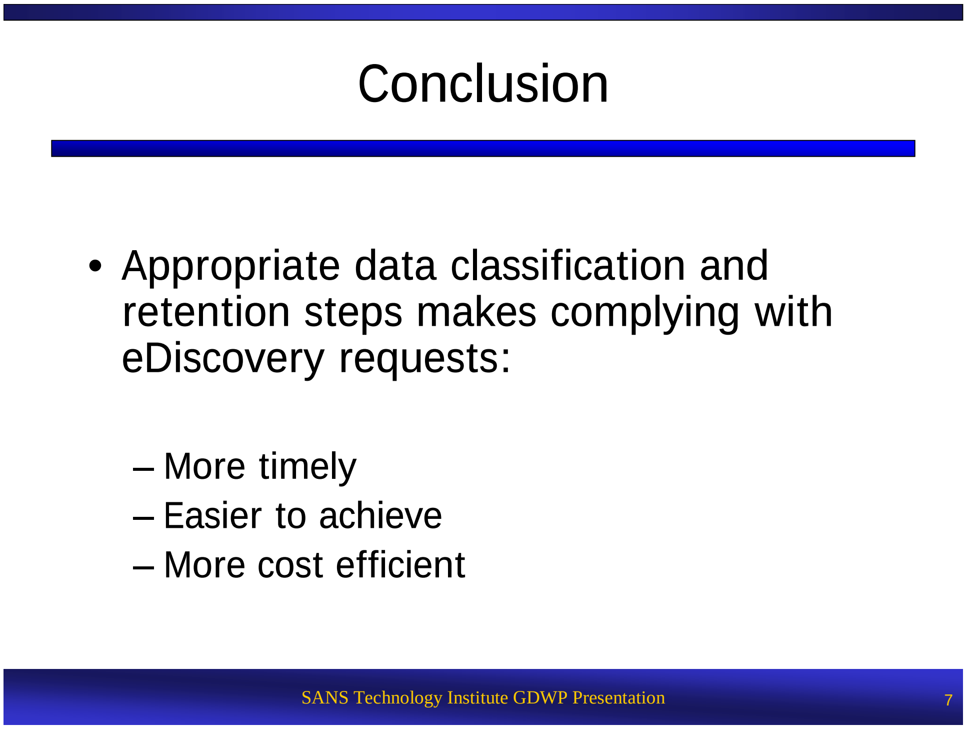
Data Labels should be used to classify data. Please see the Data Label Policy.



Data Collection Standards

- Data is kept in two secure locations
- Primary data is not to be stored on desktops, laptops or other media
- Data is housed in designated systems
- Backups are preformed according to security policy
- All of the above contribute cost effective eDiscovery

SANS Technology Institute GDWP Presentation 6



Conclusion

- Appropriate data classification and retention steps makes complying with eDiscovery requests:
  - More timely
  - Easier to achieve
  - More cost efficient

SANS Technology Institute GDWP Presentation 7

7 References

7.1 References

Trent Henry, E-Discovery: No More Losing Needles in the Electronic Haystack, Burton Group. Mar 2007

Wikipedia – Wikipedia.org

Bob Blakley, Information Classification: The Most Important Security Thing You're (Still) Not Doing, Burton Group. Mar 2007

Jonathan Sablone, Esq., Not Your Father's Keeper Deposition, Nixon Peabody LLP

Information Security Policies and Procedures, Experian, 2007

Candace A. Blydenburgh, Picking and Preparing Your Corporate Witnesses for Rule 30(b)(6) Depositions, McGuire Woods