



INFORMATION
ASSET
PROTECTION
DRAFT GUIDELINE

This draft guideline has been placed on the ASIS Guideline Web page to provide for a public review and comment period. This public review and comment period will run for 60 days from December 11, 2006 until February 14, 2007. To submit comments, one must complete the [comment form](#). Should you have questions, please email guidelines@asisonline.org.

ASIS International (ASIS) disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

This Guideline is not intended to be, and shall not be construed as, a mandatory standard of care. It does not purport to establish, nor does it establish, any industry standard or standard of due care. This Guideline has been developed by consensus, by a not-for-profit, voluntary membership organization and, as such, does not have the force of regulations or guidelines issued by governmental agencies.

This guideline does not purport to address, nor could it address, all possible remedies or methodologies. Compliance with this guideline does not necessarily prove due care, nor does non-compliance with, or disregard of, this guideline necessarily prove negligence. Security is situational. The efficacy of any security program is driven by a range of situational parameters. Practitioners must be knowledgeable about the industry and federal, state, or local laws (including case law) applicable to the jurisdiction(s) in which they practice and to the particular situation.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

Copyright 2006 by ASIS International

ISBN X-XXXXXX-XX-X

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

10 9 8 7 6 5 4 3 2 1



Information Asset Protection *Draft* Guideline

1.0	Title.....	5
2.0	Revision History.....	5
3.0	Commission Member.....	5
4.0	Committee Members.....	5
5.0	Guidelines Designation.....	5
6.0	Scope.....	5
7.0	Summary.....	6
8.0	Purpose.....	6
9.0	Key Words.....	6
10.0	Terminology.....	7
11.0	Information Asset Protection Policy.....	8
11.1	General Framework for an Effective Policy.....	9
11.2	Information Asset Protection Policy Statement.....	11
11.3	Risk Assessment Considerations.....	11
12.0	IAP Policy Implementation and Recommended Practices.....	12
12.1	Identifying Information Assets.....	12
12.2	Valuating Information Assets	12
12.3	Classifying Information Assets.....	12
12.4	Labeling Information Assets.....	12
12.5	Need to Know Controls.....	12
12.6	Privacy Protection.....	13
12.7	Information Security Awareness and Training.....	13
12.8	Key Projects and Other Potentially Competitive Information.	13
12.9	Investigating Loss or Compromise.....	14
12.9.1	Investigation.....	14
12.9.2	Damage Assessment	14
12.9.3	Root Cause Analysis.....	15
12.10	Handling, Receipt, Transmission, Storage, and Destruction.....	15
12.11.0	Protection of Information in Hard Form (Physical Product).....	16
12.11.1	Prototypes and Models.....	16
12.11.2	Manufacturing Processes and Equipment.....	16
12.11.3	Compartmentalization and Physical/Visual Barriers.	16
12.11.4	Preventing and Detecting Counterfeiting and Illegal Copying....	17

- 12.12 Technical Security Controls..... 17
 - 12.13 Technical Surveillance Countermeasures (TSCM)..... 17
 - 12.14 Information Systems Security..... 18
 - 12.15 Network Intrusion Detection and Extrusion Prevention Systems..... 18
 - 12.16 Firewalls..... 19
 - 12.17 Logical Network Access Control..... 19
 - 12.18 Application Security..... 19
 - 12.19 Sanitizing Information Systems and Media..... 19
 - 12.20 Data Security..... 19
 - 12.20.1 Encryption..... 19
 - 12.20.2 Digital Signatures..... 20
 - 12.21 The Wireless Environment..... 20
 - 12.22 Legal Protections..... 20
 - 12.22.1 Trade Secrets..... 20
 - 12.22.2 Patents..... 21
 - 12.22.3 Copyrights..... 21
 - 12.22.4 Trademarks and Service Marks..... 21
 - 12.23 Agreements Protecting Information..... 21
 - 12.24 Protecting Information in Special Environments..... 21
 - 12.24.1 Telecommuting and Remote Access..... 21
 - 12.24.2 E-Conferencing..... 22
 - 12.24.3 Domestic and International Travel..... 22
 - 12.24.4. Trade Shows..... 23
 - 12.24.5 On- and Off-Site Meetings..... 23
 - 12.25 Outsourcing to Providers..... 24
 - 12.25.1 Contractor and Subcontractor Relationships..... 25
 - 12.26 Cell Phones, Laptops, and PDA's..... 26
- 13.0 References/Bibliography..... 27
- 14.0 Appendix A Sample Policy on Information Asset Protection 30
- 15.0 Appendix B Quick Reference Guide..... 36

1.0. TITLE

The title of this document is Information Asset Protection (IAP) Guideline.

2.0. REVISION HISTORY

Baseline Document.

3.0. COMMISSION MEMBERS

Regis W. Becker, CPP, PPG Industries, Commission Chair
Mark Geraci, CPP, Bristol-Myers Squibb Co., Commission Vice Chair
Steven K. Bucklin, Glenbrook Security Services, Inc.
Edward G. Casey, CPP, Casey Security Solutions
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
Robert W. Jones, Praxair, Inc.
Michael E. Knoke, CPP, Express Scripts, Inc.
Daniel H. Kropp, CPP, D. H. Kropp & Associates, LLC

4.0. COMMITTEE MEMBERS

Edward G. Casey, CPP, Commission Liaison to Committee
Kevin Peterson, CPP, Innovative Protection Solutions, LLC, Committee Chair
Richard J. Heffernan, CPP, CISM, R. J. Heffernan & Associates, Inc., Committee Vice Chair
Ken D. Biery, Jr., CPP, CISSP, CISM, Covestic, Inc.
William R. Halliday, Marsh & McLennan Companies
Robert J. Johnson, National Association for Information Destruction, Inc.
Louis A. Magnotti III, U. S. House of Representatives
John E. McClurg, Honeywell International
Alan M. Nutes, CPP, Gulfstream
Frank E. Rudewicz, CPP, UHY Advisors
James R. Wade, CISSP-ISSAP, ISSMP, CHS-III, International Information Integrity Institute
Reginald J. Williams, CPP, CISSP, The Boeing Company

5.0. GUIDELINES DESIGNATION

This guideline is designated as ASIS GDL IAP 02 2007.

6.0. SCOPE

The scope of the Information Asset Protection (IAP) Guideline is broad in that it can be applied to all sizes of organizations and all industry sectors to include non-profits, educational institutions, and government agencies. The guideline can aid employers in developing and implementing a comprehensive risk-based strategy for information assets protection. Such a strategy may include the fundamental concepts of (1) classifying and labeling information, (2) handling protocols to specify use, distribution, storage, security expectations, declassification, return, and destruction/disposal methodology, (3) training, (4) incident reporting and investigation, and (5) audit/compliance processes and special needs (disaster recovery).

7.0. SUMMARY

This guideline is organized into three primary sections. The first section offers a general framework and some guiding principles for developing an effective Information Assets Protection (IAP) policy within any organizational setting. The second section proposes recommended practices that may be applied in the implementation of a high-quality IAP program. The third section consists of two appendices that provide useful tools for any size organization. **Appendix A** consists of a Sample Policy on IAP. **Appendix B** is a Quick Reference Guide, a sample flow chart for assessing information protection needs that can be modified and customized to meet an organization's needs.

8.0. PURPOSE

An organization's competitive edge often is the result of information derived from the creativity and innovation of its personnel. Consequently, the loss of this information would negatively impact the organization's investment in personnel, time, finances, product, and/or property. Whether it is a trade secret, patent information, or other intellectual property; a simple improvement in the way an organization produces a product or conducts its business; a technical modification, new technique, or management concept; or employee/personnel human resources information, the importance of these assets cannot be underestimated. In order to safeguard its information assets, an organization should establish a policy that requires specific measures be taken to protect information assets. This policy should outline organizational roles, responsibilities, and accountabilities, since it will be critical to the defense of an organization should a regulatory or legal matter ensue. The policy should be defined in terms that are easily understood and maintained.

Effective protection of information assets, whether in electronic, verbal, written, or any other form, involves these basic principles:

1. Classification and labeling information.
2. Handling protocols to specify use, distribution, storage, security expectations, declassification, return, and destruction/disposal methodology.
3. Training.
4. Incident reporting and investigation.
5. Audit/compliance processes and special needs (disaster recovery).

9.0. KEY WORDS

Assets, Copyright, Intellectual Property Rights (IPR), Patent, Proprietary Information, Risk, Risk Assessment, Threat, Trade Mark, Trade Secret, Vulnerability.

10.0. TERMINOLOGY

The terms defined below are for the purposes of understanding their usage within this guideline.

Assets: Any real or personal property, tangible or intangible, that a company, organization, or individual owns that can be given or assigned a monetary value. Intangible property includes such things as goodwill, reputation, proprietary information (both tangible and intangible), and related property. For purposes of this guideline, people are included as assets.

Confidentiality: Secrecy, the state of having the dissemination of certain information restricted.

Copyright: A property right in an original work of authorship (including literary, musical, dramatic, choreographic, pictorial, graphic, sculptural, and architectural work; motion pictures and other audiovisual works; and sound recordings) fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform, and display the work.

Intellectual Property Rights (IPR): A category of intangible rights protecting commercially valuable products of the human intellect. The category comprises primarily trademark, copyright, and patent rights, but also includes trade secret rights, publicity rights, moral rights, and rights against unfair competition. (Note: Some areas of the world differ significantly in their recognition and enforcement of patents, trademarks, copyrights, and other IPR. It is important to understand the IPR climate and the ability of the legal safeguards that are applicable in each jurisdiction where there is a necessity to support your business requirements.)

Non-Disclosure Agreement (NDA): A legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. In other words, it is a contract through which the parties agree not to disclose information covered by the agreement.

Patent: Information that has the government grant of a right, privilege, or authority to exclude others from making, using, marketing, selling, offering for sale, or importing an invention for a specified period (20 years from the date of filing) granted to the inventor if the device or process is novel, useful, and nonobvious.

Proprietary Information: As defined by the Federal Acquisition Regulation (48 CFR 27.402 Policy): A property right or other valid economic interest in data resulting from private investment. Protection of such data from unauthorized use and disclosure is necessary in order to prevent the compromise of such property right or economic interest.

Risk: A security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.

Risk Assessment: A systematic process whereby assets are identified and valued, credible threats to those assets are enumerated, applicable vulnerabilities are documented, potential impacts or consequences of a loss event are described, and a qualitative or quantitative analysis of resulting risks is produced. Risks are generally reported in order of priority or severity and attached to some description of a level of risk.

Root Cause Analysis: A technique used to identify the conditions that initiate the occurrence of an undesired activity or state.

Sensitive Information: Information or knowledge that might result in loss of an advantage or level of security if disclosed to others.

Service Mark: A name, phrase, or other device used to identify and distinguish the services of a certain provider. Service marks identify and afford protection to intangible things such as services, as distinguished from the protection already provided for marks affixed to tangible things such as goods and products.

Technical Surveillance Countermeasures: Employment of services, equipment, and techniques designed to locate, identify, and neutralize the effectiveness of technical surveillance activities.

Threat: The manifestation of an ability or intent to adversely affect an asset.

Trade Mark: A word, phrase, logo, or other graphic symbol used by a manufacturer or seller to distinguish its product or products from those of others.

Trade Secret: All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processed, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (a) the owner thereof has taken reasonable measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

Vulnerability: A weakness or organizational practice that may facilitate or allow a threat to be implemented or increase the magnitude of the impact of a loss event.

11.0. INFORMATION ASSET PROTECTION (IAP) POLICY

As with implementation of any successful organizational policy, it is essential that at the outset of discussions concerning an Information Asset Protection (IAP) policy that:

1. An organization's leadership provide commitment, budgetary resources, and depth of support so all business units assume appropriate responsibility for developing strategies to align organizational and protection goals.
2. A dedicated department, group, and/or individual(s) be tasked with the responsibility for the policy management and overall accountability/audit.
3. All business units, personnel, temporary employees, vendors, consultants, contractors, and business partners be required to adhere to the policy.

4. Continuous education and training be conducted for the affected parties.

11.1. General Framework For An Effective Policy

Ultimately, the responsibility for protecting information assets rests with the leadership of an organization. When they exist in an organization, departments such as security, legal, operations, human resources, information technology, and other functions often assist in developing, implementing, and supporting the effort. Some of the roles and responsibilities for managing an IAP policy include the following:

- Ensuring that risk identification, evaluation, and mitigation activities are integrated into and support business processes.
- Developing, implementing, and managing a program of integrated protection controls to mitigate identified risks to an acceptable level.
- Identifying cross-sector interdependencies of information asset and physical asset protection.
- Ensuring that information technology (IT) systems and telecommunications systems complement the IAP policy.
- Defining and communicating roles and responsibilities and adherence to roles and responsibilities throughout the organization and with employees, partners, vendors, suppliers, consultants, customers, etc.
- Performing regular internal assessments of the policy.
- Tracking security events and conducting post-event reviews to identify root causes and determining if protection measures fit the originally intended purposes and are consistent with the current risk profile.
- Reporting significant changes in risk and/or asset value to appropriate levels of management on periodic and post-event basis.
- Defining a process for formal risk acceptance by management.
- Assigning responsibility to monitor potential changes in contractual obligations, regulations, laws, and intellectual property rights issues in order to assess potential impact on the organization.
- Identifying and communicating unique regional or site issues, cultural, legal, or organizational requirements and assessing potential impact to the organization.

Information assets may include all forms and types of financial, business, and scientific information, customer related information (including identification, preferences, and pricing), business strategies, manufacturing processes, research and development, personnel data, etc. Such information may be electronically generated and processed, stored on some form of storage media, printed on paper or on other mediums whereby information may be recorded and communicated.

Failure to take reasonable steps to protect assets from unauthorized use may make it difficult for an organization to obtain legal recourse in preserving its intellectual property rights if the information is compromised.

It is important to identify what information should be protected and then identify the many forms this information may take over its lifecycle. It is also important to recognize that only a certain segment of the organization's information may warrant protection. Once such information is identified, it should be classified such that the most significant information assets receive the

greatest degree of protection. However, some suggested controls might not be applicable, or practical, in every part of every organization. Failure to include appropriate subject matter expertise at the beginning of project discussions and design can result in significantly increased security costs and the potential for less effective solutions.

An organization’s leadership should consider both the *categories* of information and the *levels* of information that represent protection objectives.

Categories of information assets may include:

◆ Proprietary Information (Customer lists, marketing plans, pricing strategies, test results, etc.)	◆ Physical Products (Prototypes, models, molds, dyes and manufacturing equipment, etc.)
◆ Trade Secrets	◆ Trade Marks and Service Marks
◆ Patent Information	◆ Privacy Information (Personal data, evaluations, credit info, etc.)
◆ Copyright Information	◆ Regulated Information (Health Information ¹ , financial data, government classified, etc.)

Although the controls outlined in this section of the guideline are primarily designed for protecting proprietary and trade secret information, they serve equally well for all information assets including those listed above.

Levels of information may be determined by criteria such as:

Sensitivity. This information includes that which if disclosed outside of trusted people and processes would likely have a significant impact on the organization’s operations and business strategy.

Criticality. Critical information is that upon which an organization relies to accomplish its mission and support business decisions.

Other levels and/or terms are commonly used in various business and organizational settings to distinguish the degree of sensitivity or degree of protection warranted. These include confidential, restricted, limited, non-public, and others. Most organizations define between two and four levels of sensitivity/protection. Fewer than two levels may not adequately distinguish material, and more than four levels may be too complicated and cumbersome to effectively manage.

It should be noted that some information might require protection only for specific periods of time. An example of this can be found with the National Aeronautics and Space Administration (NASA) during a typical space shuttle launch. Prior to and during a shuttle mission, certain

¹ Such as protected information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

information is considered highly sensitive. Once the mission is completed, some of that information becomes obsolete or no longer requires the same level of protection. Similarly, efforts to protect patent information can often be minimized once the patent has expired.

11.2. Information Asset Protection Policy Statement

The policy statement sets the tone for the organization, its employees and all those in a trusted relationship (e.g., consultants, sub-contractors, partners, and vendors). In addition, being able to demonstrate a meaningful, well-communicated and consistently enforced policy often helps to support any subsequent legal actions if they become necessary.

The policy should present a general introductory statement based on the premise that:

- Information is one of the organization's most important resources.
- All information needs to be appropriately evaluated according to its sensitivity.
- Protection measures should be sufficient to ensure confidentiality, integrity, availability, accountability, recoverability, auditability, and non-repudiation for information in both the physical and cyber environment.

(See Appendix A, Sample Policy.)

11.3. Risk Assessment Considerations

A thorough and tailored risk assessment is the foundation in the development of an overall IAP strategy. Questions such as the following are often helpful in performing a risk assessment:

- What competitive advantage does this information provide?
- What is the likelihood that competitors are seeking this information?
- What is the potential damage to the organization's operations?
- What is the potential damage to an individual?
- What is the potential damage to the organization's reputation or image?
- What is the potential for loss of customer, shareholder, or business partner confidence?
- What is the potential for loss of trade secret or patent protection?
- What is the potential for loss of ability to be first to market?
- What is the potential for loss of market share?
- What is the effect on stock value or venture capital support?

Assessments should be performed on a regular basis to address changes that may occur in the business environment, security requirements, and the nature of the information assets, threats, vulnerabilities, and impacts. In addition, they should be performed in a systematic manner such that the process and results are reproducible. These assessments, in certain circumstances, may include the inclusion of appropriate IPR risk assessments as part of a due diligence process prior to any business transaction. These assessments need to be product, technology, and transaction specific in order to be most effective at identifying, assessing, and addressing risk.

Please see the ASIS General Security Risk Assessment Guideline, available at www.asisonline.org/guidelines/guidelines.htm, for further information on how to conduct a risk assessment.

12.0. IAP POLICY IMPLEMENTATION AND RECOMMENDED PRACTICES

The following principles form the foundation of an effective IAP policy: identifying, valuating, classifying, and labeling information assets; need-to-know controls; privacy protection; security awareness and training; information asset management; and investigating loss or compromise. This section provides general guidance -- in a "how-to" format -- for implementing an effective IAP program in organization. Each subsection lists practices and/or procedures that should be considered as part of an overall protection strategy. For many of these issues, more specific information is available in the resources listed in the References/Bibliography section.

12.1. Identifying Information Assets

The first step in implementing an IAP is to identify the information that may need to be labeled and protected. This step helps narrow the scope of the information that requires protection and focuses limited security resources where they are most needed.

12.2. Valuating Information Assets

After information is identified, an organization needs to perform a valuation process to determine importance and criticality to the enterprise.

12.3. Classifying Information Assets

An organization must establish a classification system that assigns a value to critical information. (See Appendix B.)

12.4. Labeling Information Assets

All identified assets should prominently display the appropriate classification and level in whatever media it appears.

12.5. Need-To-Know Controls

- An employee's access should be based on his or her current job function and a need-to-know basis, not solely on a position or management level.
- Use categories and levels of information to aid in defining need-to-know controls.
- Apply methods/layers of protective measures to information assets appropriate to their categories and levels.
- Ensure that successive methods/layers of protective measures complement the organization's overall policy and provide the balance between the conduct of the business and approved accessibility.

12.6. Privacy Protection

In addition to proprietary and trade secret information, all organizations handle some form of “privacy” information pertaining to their employees, management, relationships, customers or others. In order to maintain the necessary level of trust and to meet legal and regulatory requirements, distinct controls on privacy information should be implemented.

- Establish specific privacy policies and designate an employee responsible for implementing and managing the privacy program.
- Evaluate privacy information relating to employees, partners, vendors, customers, and others and determine legal and regulatory requirements.
- Ensure systems are in place to ensure employee privacy is not compromised.
- Review applicable federal, state and international guidelines to ensure adequate internal controls are in place to protect the privacy of employees.²
- Clearly mark privacy information properly released to indicate:
 - How the information will be used and made available to others.
 - Proper notifications and actions if a compromise should occur.
 - Destruction or disposition instructions when the information is no longer needed.
- Conduct program audits to ensure privacy policies are practiced effectively.

12.7. Information Security Awareness and Training

Almost invariably, security awareness and training is one of the most cost effective measures that can be employed to protect corporate and organizational information assets. This is largely due to the fact that protecting information, generally more so than any other asset, is best achieved through routine business practices that permeate every element of an organization. Therefore, where each individual entrusted with sensitive information takes prudent measures and personal responsibility for protecting those assets, a robust security environment should occur naturally.

- Determine the need for and scope of an Information Security Awareness Training program within the organization based on a comprehensive risk assessment and the nature of the business.
- Consider developing and delivering tailored security awareness training for all individuals in a trusted relationship.
- Include non-employees such as part-time personnel, temporary employees, consultants, sub-contractors and on-site vendors in such training.
- Deliver awareness training on a recurring basis and via multiple modes to effectively reach all appropriate personnel.
- Whenever possible, information security awareness and training should be documented.

12.8. Key Projects and Other Potentially Competitive Information

- Consider requiring specific information asset protection policies for key projects, initiatives, new product lines, etc.

² Additional guidance is available at the Federal Trade Commission Web Site, www.ftc.gov/privacy and from the European Union (EU) Data Protection Directives.

- Ensure that peripheral information, such as supply orders, hiring needs, facility enhancements, etc., observable activities, or other indicators do not provide valuable intelligence to a competitor or adversary.
- Consider the vulnerability of information released to outside entities as part of joint ventures, partnering agreements, or trusted partner (vendor, supplier, client) arrangements. Recognize that the other entity may not have the same level of protective measures in place for information that your organization considers adequate.
- Consider publicly available information in the aggregate, not just item by item.
- Assess potential vulnerabilities by taking the adversary's perspective and defend against realistic collection techniques.
- Coordinate major releases with all relevant elements of the organization including marketing/public relations, human resources, budget and finance, production, research and development, and others as appropriate.
- A pre-release approval process should exist for any presentations, papers, or articles that may contain information pertinent to sensitive activities or plans.
- Periodically review Web content concerning the organization (and the sites of joint ventures, partnering agreements, or trusted partner [vendor, supplier, client]) and key projects to assess publicly available information.

12.9. Investigating Loss or Compromise

Investigations contribute not only to subsequent litigation and support to law enforcement agencies (if appropriate), but also to asset recovery, identifying the root cause of the incident, preventing future occurrences, assessing the real damage or loss caused by the incident, identifying peripheral issues/problem areas, and recommending corrective actions. Appropriate investigative techniques should be used at all times and legal considerations taken into account when developing an investigative plan.

12.9.1. Investigation

- Establish an investigative plan and coordinate with counsel.
- Thoroughly investigate known and suspected compromises of information.
- Identify investigative resources that are available (both internal and external) or may be needed including forensic laboratory support and various expert capabilities.
- Establish and maintain effective liaison relationships with law enforcement and investigative service providers as well as various information sources.

12.9.2. Damage Assessment

- To the extent possible and as soon as possible, determine exactly what information has been compromised.
- Determine the implications of the compromise in terms of economic loss, research/project delays, operational impact, corporate image, shareholder confidence, legal liability, and corporate relationships (partners, vendors, suppliers, subcontractors, etc.).
- Determine the actual and potential impact of the compromise on other corporate projects and initiatives.
- Report actual and potential impact to an appropriate level of management.

12.9.3. *Root Cause Analysis*

- Attempt to identify any systemic problems or existing business practices that would allow or contribute to the compromise of sensitive information.
- Maintain easily accessible documentation (or an automated database) on incidents (including allegations and suspected incidents) related to the compromise or suspected compromise of sensitive information. This is extremely valuable for Root Cause Analysis subsequent to a known compromise and for historical trend analysis. It is also useful in determining the aggregate information that has been released over time on a particular project or initiative.
- Following a root cause analysis, identify and implement appropriate corrective actions and follow-up to adjust policies and practices that contributed to or facilitated the loss incident.

12.10. Handling, Receipt, Transmission, Storage, and Destruction

- Enforce access restrictions according to sensitivity level of the information and “need-to-know” criteria for individuals.
- Shredders or secure collection receptacles should be conveniently located near office areas with printers, copiers, and fax machines.
- Signage should be posted in office areas with printers, copiers, and fax machines reminding employees that overruns and misprints need to be destroyed.
- Consider, where appropriate, the documenting of all transfers (internal and external) of sensitive records/documents.
- Consider conducting periodic, random audits to ensure compliance.
- Conduct and document a selection process and due diligence for any contractors that will process records, documents, or sensitive information in any manner.
- Ensure central records storage facilities comply with established fire and building codes and standards that address issues such as shelving, fire suppression, and compartmentalization.³
- Destroy records and sensitive information in a manner that precludes reconstruction consistent with its level of sensitivity; and document the date and place of destruction.
- Obsolete stored records should be destroyed regularly according to a records retention schedule.
- Destroy incidental and duplicate records on a regular basis.
- Collect and store information/media to be destroyed such that it is secured from unauthorized persons (including cleaning crews) and in containers that prevent inspection, handling, and/or removal.
- Avoid, if possible, discarding particles of destroyed media in outside trash receptacles accessible to the public or by a method where they could be retrieved.
- Protect records and information while in transport by using measures such as locked containers, seals, escorts, RFID (Radio Frequency Identification) tags, transportation logs/receipts, and other means as appropriate.
- Where appropriate, a means should be employed to distinguish original documents from reproductions - and in some cases, reproduced copies should be numbered and accounted for.

3. “Compartmentalization” in this context refers to limiting the amount of materials in any space or area that is not separated by a mechanism to prevent or substantially inhibit the spread of fire. In this case, the National Fire Protection Association has determined that no more than 250,000 cubic feet of records should be in any area or space that is not separated by an adequate firebreak mechanism.

- Minimize unnecessary retention of sensitive records and materials by periodically reviewing the need to retain information, including duplicate copies, and enforcing an effective destruction policy.

12.11. Protection of Information in Hard Form (Physical Product)

12.11.1. *Prototypes and Models*

- Prototypes and models should be afforded all the same physical security, access controls, classification, employee vetting, verification, and documentation as other information assets. Particular attention should be paid to prototypes and models whether they exist in the form of paper designs, hardware, test vehicles, market test materials, software, or other prototypes.
- Obsolete prototypes, models, and test items should be destroyed such that they may not be reversed engineered.
- Contractors or vendors entrusted with prototypes, models, or test items should be contractually bound to protect them in a manner consistent with the owner's policies and procedures; and they should be provided with instructions for return or disposition of the items when no longer needed.

12.11.2. *Manufacturing Processes and Equipment*

- Access to production or processing facilities should be restricted to those employees that require access to perform their functional responsibilities.
- Prohibit unauthorized photography within the production or processing areas.
- Contractors with access to the production or processing area should have executed NDA's such as those required for the handling of other sensitive information assets.
- Employees, contractors, and visitors entering the production or processing area should sign in using a control system (or log), and display clearly visible identification badges indicating their status and approved level of access.
- Obsolete and/or damaged production equipment, as well as scrap, should be disposed of in a manner that does not compromise or divulge information regarding the production or processing area (e.g., the amount or scrap magnesium generated may indicate production levels of certain products).
- Consider, where appropriate, protecting information regarding loading dock activity, deliveries, and shipments.

12.11.3. *Compartmentalization and Physical/Visual Barriers*

- Information of various classifications should not be co-mingled but should be compartmentalized with increasing levels of security to match increasing levels of sensitivity.
- Safeguards such as barriers and covers should be employed where sensitive information may be visually exposed to unauthorized individuals (when in place and during transport).

12.11.4. Preventing and Detecting Counterfeiting and Illegal Copying

- Monitor Internet activity on a regular basis to identify potential counterfeit products, sales, similar products, as well as other suspicious activity.
- Conduct training sessions with employees to alert them about similar products and potential counterfeited products and backgrounds of known suspects, competitors, or common schemes.
- Require all employees, vendors, and subcontractors to sign non-disclosure agreements (NDA's).
- Design in and employ unique packaging, product type, and/or shape to prevent re-labeling, re-pricing, etc.
- Employ appropriate anti-counterfeiting technology consistent with a security risk assessment.
- Maintain strict numbering and sequence control markings for all technical memoranda and reports.
- Develop protocols for regular compliance and inventory control audits of internal and external relationships.
- Create aggressive Internet communication and education strategies to raise awareness, educate, inform, and collect intelligence.
- Maintain close liaison with law enforcement and prosecutorial agencies to assist in detection, awareness, alerts, and information sharing efforts.
- Consider participation in programs such as the U.S. Customs Intellectual Property Rights e-Recordation program. <https://apps.cbp.gov/e-recordations/>
- Understand jurisdictional requirements to register IPR.

12.12. Technical Security Controls

This section incorporates steps to mitigate technical collection threats and measures related to Information Technology (IT) security. Incorporating more traditional protection measures with these technical issues and associated controls truly represent an application of the principle of “convergence” in asset protection. Many of the approaches described in this section require specialized expertise, and some services may need to be outsourced. Be sure to select outsourcing partners carefully and perform solid due diligence on prospective providers, as you will be establishing a strong trust relationship with them.

12.13. Technical Surveillance Countermeasures (TSCM)

A key element of the threat to sensitive information involves technical means of collection by adversaries. Technical Surveillance Countermeasures (TSCM) refers to the use of services, equipment, and techniques designed to locate, identify, and neutralize the effectiveness of technical surveillance activities (electronic eavesdropping, wiretapping, bugging, etc.). Technical surveillance countermeasures should be a part of the overall protection strategy. Individuals within the organization responsible for physical security, facility security, information asset protection, telecommunications, meeting planning and information technology all have a stake in addressing these concerns.

- Regularly inspect telecommunications equipment, cables, and terminals for technical surveillance compromises using equipment, methodologies, and personnel capable of detecting current threats.
- Offices and meeting rooms should be regularly inspected for technical surveillance vulnerabilities on a random basis and also immediately prior to any sensitive or proprietary discussions.
- Use credible and trusted service providers for technical countermeasures support. Be sure to perform a thorough screening process before engaging a particular vendor.
- Perform periodic scans for unauthorized wireless network devices, regardless of whether a wireless network is installed.

12.14. Information Systems Security

Information systems security includes controls that protect information systems such as networks and standalone systems. Protections are needed for the network perimeter, internal network components, communications, applications, data, and end user devices.

- Consider how IT controls will impact the organization's ability to implement emergency, safety, and business continuity measures.
- Change default manufacturer passwords, user names, and administrative accounts.
- Assign administrative privileges appropriately. Administrators should use non-privileged accounts when not performing system administration. Administrative and user accounts should not be group accounts whenever possible.
- Limit and monitor physical access to network components.
- Install and update anti-virus and firewall software on network servers and client devices (laptops, workstations, and personal electronic devices).
- Train users in computer security awareness, including the risks associated with remote access, mobile access, and wireless technology.
- E-Commerce: Implement adequate security controls and methodologies to ensure internal resources are not compromised by Internet-related activities or services.
- Require external organizations with access to information systems maintain an equivalent security posture through compatible security practices. This requirement should be added to contracts and service agreements.
- Combine IT security controls, such as firewalls and Intrusion Detection Systems to provide multiple layers and methods to stop possible attacks.

12.15 Network Intrusion Detection and Extrusion Prevention Systems

NOTE: Sections 12.16 through 12.20 highlight several technical IT security measures that can be considered. Since these measures are technical, a limited description is presented. It is recommended that you work with your internal IT organization or individual to determine which of these measures should be implemented. Key factors to consider are the amount of information within your company that is considered an information asset and the level of protection that this information should receive.

Intrusion Detection Systems (IDS) monitor for malicious programs and unauthorized changes to files and settings. They also monitor network traffic and provide real-time alarms for network-

based attacks. Extrusion Prevention Systems can be configured to prevent the unauthorized transfer of critical information via e-mail, Internet, or other communications methods.

12.16. Firewalls

A firewall should be used to protect the boundaries of the network by filtering communications. The firewall blocks or redirects unauthorized or potentially dangerous information (packets, files, email, etc.), notifies system administrators to critical incidents, and logs attempted intrusions for automated or manual analysis.

12.17. Logical Network Access Control

Logical network access control is the process by which users are identified and granted privileges to information, systems, or resources. The primary objective is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources.

12.18. Application Security

Modern business applications typically consist of custom code, third party software components, and one or more servers. Improper integration of these components can sometimes result in a vulnerability that can later be exploited to gain unauthorized access to your data. Even with strong network security, application level attacks have proven that vulnerabilities could be exploited using a point of entry legitimately open for business needs.

12.19 Sanitizing Information Systems and Media

Sanitizing is the process of removing the data on the media before the media is reused. In general, laboratory techniques cannot retrieve data that has been sanitized/purged. Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Clearing is the process of eradicating the data on the media and can be accomplished by overwriting or degaussing (reducing or eliminating an unwanted magnetic field). In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval. Destroying is the process of physically damaging the media to the level that the media is not usable as media, and so that there is no known method of retrieving the data.

12.20 Data Security

These measures are designed to protect the information (or data) while it is being processed, stored, or transmitted by IT or other electronic systems.

12.20.1 Encryption

Encryption involves obscuring the meaning of a piece of information by altering or encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. Encryption should support an information identification, classification, and protection structure.

12.20.2. Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message. Digital signatures are especially important for electronic commerce and e-mail.

12.21. The Wireless Environment

Wireless Local Area Networks (WLAN's) can provide a cost effective method for accessing an organization's network. WLAN's can be used as an alternative to or an extension of traditional wired networks, especially in those areas that create a difficult installation of these infrastructures. However, WLAN's can introduce significant risks if not properly installed, configured, and monitored. Your IT organization or individual is the best resource to understand and mitigate these risks.

12.22 Legal Protections

Various definitions of terms such as "intellectual property" and "trade secret" apply in different settings, including at the federal versus the state/local level in the United States. The Economic Espionage Act defines these terms at the federal level, while various definitions exist at the state level, often based on the definition found in Black's Law Dictionary. In general, the elements of a trade secret include some form of the following: economic value or advantage to the holder; clear identification of the information; and reasonable and prudent protection measures. Legal actions and assets protection strategies should carefully consider the venue (or venues) in which any legal action may take place and, hence, the applicable laws and definitions. Listed below are areas to discuss with your organization's legal counsel.

- Taking enforcement actions on any patent, copyright, or trademark/service mark violations.
- Understanding current legal protocols and case law to assist in determining lost profits and financial damages and ascertaining appropriate protection strategies.
- Understanding the status of intellectual property rights protection and the nature of violations in each jurisdictional where the organization plans to do business.
- Evaluating the effectiveness of IPR protections in each country to ensure control currently and in the future.
- Participating in programs such as the U.S. Customs Intellectual Property Rights e-Recordation program. <https://apps.cbp.gov/e-recordations/>

12.22.1 Trade Secrets

- In order to be able to prove a trade secret case in court, document your identification and valuation of the asset, its role in establishing competitive advantage in your industry, and the full scope of protection measures you have instituted to protect it.
- Ensure that reasonable and prudent traditional and cyber security measures are in place to prevent unauthorized access to trade secrets.
- Conduct periodic, random security audits to ensure compliance.
- Execute NDA's with employees, suppliers, and consultants, etc. prior to any disclosure.
- Establish need-to-know criteria to ensure individuals have access to only the specific information they need in order to do their jobs.
- Institute effective information warning notifications to ensure individuals are aware of exactly what needs to be protected.

- Take steps to properly destroy materials no longer needed to prevent compromise.

12.22.2 Patents

- Follow trade secret guidelines for all newly discovered processes/products until a patent has been issued.
- Establish a patent strategy to ensure that patent protection is acquired in all appropriate jurisdictions.

12.22.3 Copyrights

- Apply copyright markings to original works.
- Register materials to be copyrighted in all appropriate jurisdictions.

12.22.4 Trademarks and Service Marks

- Apply appropriate trade/service markings and notices to materials produced by the company.
- Register trade/service marks for processes and products in all appropriate jurisdictions.

12.23 Agreements Protecting Information

Written non-disclosure agreements assist in ensuring a common understanding as well as a legal obligation with respect to protecting information assets. NDA's should acknowledge that any information on any media that records business communications or transactions is considered an official record under the law and will be handled in a manner consistent with the policies and procedures regarding other information assets.

- All employees should execute an NDA as a condition of employment. Via the agreement, the individual should acknowledge that all information assets regarding the employer, vendors, and customers are considered confidential, will be kept confidential, and are the property of the employer.
- Employee NDA's should also include verification that the employee has read, understands, and will abide by the IAP policies and procedures.
- A contractor, subcontractor, consultant or vendor that has access to information assets in any form and for any purpose should be contractually bound to protect the information to the same degree as they are protected in-house, and commensurate with the asset's level of sensitivity.
- Employees should be debriefed upon resigning or termination, and should be reminded of their continuing obligations under the NDA.

12.24 Protecting Information in Special Environments

There are a wide variety of special circumstances and environments that pose unique or additional requirements/considerations in terms of information asset protection. Some of the most common are mentioned here.

12.24.1 Telecommuting and Remote Access

Users connect to the company's private network using various technologies so the network architecture must include alternative connection methods. A Remote Access Server (RAS)

provides remote network access via modem while using basic user defined or domain specified account authentication. Remote users can connect to an enterprise network through the Internet using an encrypted virtual path. Since the RAS connections are point to point, no encryption is required.

- Strong authentication and encryption are required, especially for remote access to privileged and administrative information.
- Disconnect wireless or LAN connections prior to connecting to an RAS.
- Strong monitoring and auditing of remote access traffic is critical.

12.24.2 E-Conferencing

Holding meetings and other communications using video, telephone, and web-based technology is a very popular and even critical element of successful business and organizational dealings. Unfortunately, the telecommunications infrastructure and the Internet weren't designed to be secure. Regardless of its lack of security, business and organizations are using these mediums to communicate sensitive and private information that is critical to their operations.

- Understand how a service provider deals with private information and what policies have been implemented to ensure the data is protected at all times.
- It is important to find out what the service provider's policy is regarding passwords. A mechanism should be in place to address password maintenance. It is also critical to know who at the service provider has access to passwords.
- Whenever possible, encryption should be used for the transfer of data and when feasible, passwords should be scrambled through encryption.
- Use access control mechanisms and encryption when discussing sensitive data.
- Unless the security measures can be validated, users should assume their discussions are not private.

12.24.3 Domestic and International Travel

Special circumstances, threats, and vulnerabilities may arise during business travel. Consider these issues prior to travel. There are several services - including the US Department of State's Overseas Security Advisory Council (OSAC) - able to assist in travel and destination risk analysis. Effective planning and preparation will aid in mitigating associated risks.

- Business travelers, especially those who will be involved with any form of sensitive information assets, should:
 - Receive a pre-travel security briefing and/or consult travel advisories, notifications, information services, and publications prior to departure.⁴
 - Use organizational recommendations for travel agencies to facilitate tracking and itinerary and schedule changes (especially during potential emergencies).
 - Travel with a low profile without visible identification that shows organizational, personal, or national identity to reduce one's targeting potential.

⁴ This information is available from a variety of Government and private sector sources, both online and in hardcopy.

- Restrict information carried to only what is absolutely necessary.
- Carry information with you, not in checked baggage, and do not surrender baggage containing sensitive information to baggage handlers or bellmen.
- Be aware that economic espionage targeting, including technical surveillance, is possible.
- Avoid working on or discussing sensitive information in public areas or on public transportation where information may be subject to inadvertent or deliberate compromise.
- Use computer privacy screens, cable locks, and other recommended solutions to improve information asset protection.
- Use company offices and office equipment, including computers, faxes, printers, and secured network connections, when and where available, during travel.
- Avoid use of hotel faxes, copy facilities, and business centers for sensitive information.
- If required to transfer electronic files to facilitate printing, copying, or projection of presentation materials, be sure to remove data from temp and other files on non-owned equipment.
- Follow organizational guidance concerning telecommuting.
- Report actual, attempted, or suspected targeting of information during travel.

12.24.4 Trade Shows

Trade shows offer a traditional venue for business and government intelligence collection. Corporate policy should clearly define and enforce the line between marketing activities and compromise of sensitive information. Training, awareness, and preparation are key elements of an assets protection strategy for trade show participation.

- Establish an education awareness program and a reporting mechanism tailored to individuals who travel to trade shows, conferences, symposia, and technical meetings. Education awareness programs should include up-to-date information on information asset protection, personal safety, crime prevention, travel security, elicitation techniques, etc. Travelers should also be aware of NDA's that are in place.
- Identify "high risk" travelers based on their position, project, access, or clearance within the company. Develop and implement special procedures for "high risk" travelers.
- Consider documenting all information and equipment (such as laptops, notebook computers, hand held devices, etc.) to be carried to the meeting and make backup copies of information or computer files when appropriate.
- Ensure travelers are debriefed upon their return when appropriate (e.g., high risk, overseas technical conference, etc.) Document key points and report internally and/or externally as appropriate.
- Follow-up on relevant information from debriefings, post-travel reports, and other sources relevant to travel security or information assets protection during travel.

12.24.5 On- and Off-Site Meetings

On- and off-site meetings, especially those of a business or scientific nature, have a long history of being targeted for information collection and development of relationships with attendees. Obtain an annual schedule of the organization's strategic and critical business meetings and develop a tailored IAP strategy for each meeting as necessary. It is important that a risk

assessment of scheduled meetings be used as a guide in planning appropriate security controls to help mitigate identified risks for each event.

- Perform a risk assessment for off-site meetings where information assets may be discussed or shared.
- Establish liaison with security and other departments at venue sites required to obtain floor plans and details concerning telecommunications, network, and audio/visual infrastructure and equipment prior to venue approval.
 - Work with meeting planners to identify and select meeting sites and room assignments based on information protection concerns and ability of location to support business and security requirements.
- Arrange for a low-profile event when appropriate, minimizing signage and electronic postings of events, sponsors, room locations, and schedules. Use meeting names that do not suggest subject matter or identify attendees.
- Based on the results of the risk assessment, determine the need to perform a Technical Surveillance Countermeasures inspection before and during meetings to mitigate the risk of technical collection. Vulnerabilities commonly identified include unencrypted wireless mikes, vulnerabilities with infrared and other wireless headsets used to translate language, audio leakage, devices and unplanned electronic equipment brought in by participants or others, and unsecured telecommunications equipment, cables, and terminals.
- Determine the need for secure shipment and storage before, during, and after event.
 - Maintain security of printed materials and computer media during reproduction, transportation, and storage prior to distribution.
- Limit hard copy information distributed to the extent possible.
- Insure that electronic presentations are protected during all stages of creation, editing, transmission, and presentation.
- Ensure that electronic presentations are removed from non-owned presentation computers using approved methodologies/software that prevent recovery of data.
- Ensure suppliers use information security practices supportive of organizational goals and restrict use of outside resources without security precautions.
- Determine if venue site will limit access to rooms or allow your organization to do so.
- Determine the need for security officers to control access and to provide 24-hour security of meeting rooms and electronic equipment, including laptops.
- Collect information and notes left behind by attendees, to the extent possible, for secure disposal or return or arrange for on-site shredding service by an approved provider.

12.25 Outsourcing to Providers

A wide variety of business functions are being outsourced to third-party providers including foreign entities. Asset owners should recognize that this practice transfers operational control and accountability for the business function to outside parties and may increase the risk to information assets. In certain cases, the information risks are not easily identifiable and may result from subtle or hidden clauses in contracts and outsourcing agreements. Be sure to thoroughly assess potential risks and balance business and security requirements.

- Thorough due diligence should be performed for potential outsource providers, including:

- Financial performance and reputation including IPR violations, trade complaints, or export control issues of the potential partner in past business dealings of a similar nature, including potential partner links to foreign governments or firms with intellectual property rights violations, trade complaints, or export control issues
- Full or partial foreign ownership or controls of any US-based outsource providers.
- Individual and corporate non-disclosure agreements (NDA's) should be in place with potential outsourced providers prior to discussions. Subcontractors should be identified and NDA's obtained. Ensure that no NDA's will conflict with the project.
- An initial on-site security review should be completed prior to signing an outsourcing agreement, and regular on-site security reviews should be conducted to ensure continued compliance, at locations both inside and outside the U.S.
- Advise personnel of contract requirements and identify an on-site individual(s) responsible and accountable for compliance.
- Identify, physically and logically, where personnel will work and ensure that appropriate physical security and information technology requirements are in place.
- Contact your organization's legal counsel for applicable laws and regulations (of all participating countries) concerning the export and import of technology, personal and privacy information, and implementation/enforcement of proper protection procedures to help ensure compliance.⁵

12.25.1 Contractor and Subcontractor Relationships

An organization should have security measures clearly articulated, agreed upon by all parties, and formally written into contracts, agreements, and similar legal documents.

- Contractors and subcontractors that process information in any manner (e.g., data entry, imaging, scanning, conversion, storage, and destruction) should be thoroughly evaluated. Such evaluation may include employee background screening requirements, contracts with other organizations, etc.
- Contractors and subcontractors should sign an NDA to be kept on file and include, but not be limited to, the following terms:
 - Contractors and subcontractors should be bound by an NDA that specifically delineates the policies and procedures, including all security measures, by which they will provide services for which they were hired.
 - NDA's will be completed and kept on file for all individuals who have access to project information. These agreements should indicate that the employee acknowledges and understands that all information to which he or she is exposed is not to be disclosed and that he or she may be subject to termination, criminal, and/or civil action should that agreement be breached.
 - Individuals are obligated to report any breaches of security or information compromises, as well as cooperate in any investigations.

⁵ Determining applicable laws and regulations is generally outside the scope of the security function within an organization. Nonetheless, it is an important task in the international environment and helps ensure that sensitive information is properly – and legally – protected.

- All records will be returned or destroyed in a prescribed manner upon termination of the project or when no longer needed.

12.26 Cell Phones, Laptops, and PDA's

- As a condition of issuing any portable equipment capable of generating or storing information (e.g., notebook computers, blackberries, etc.), employees should sign a release acknowledging that the equipment and any information produced or stored on it are the property of the employer.
- Use of mobile devices with embedded cameras (e.g., cell phones) should be controlled and discouraged, particularly around sensitive materials or in restricted areas.
- Avoid storing sensitive such as Social Security Numbers, credit card numbers, and passwords on any wireless device.
- Be careful about posting your cell phone numbers and email address. Attackers often use software that browse Web sites for email addresses, which then become targets for attacks.
- Do not follow links in an email or text message. Be suspicious of URL's sent in unsolicited email or text messages. While the links may appear to be legitimate, they may actually direct you to a malicious Web site.
- Consider locking your phone when not using it or creating a password for phone access. Consider installing software that allows you to remotely lock the phone or erase the data if the phone is lost or stolen.
- Asset tag or engrave the laptop. Permanently marking or engraving the outer case of the laptop with the organization's name, address, and phone number may greatly increase the odds of getting the laptop returned.
- Rename the Administrator Account.
- Prevent the last logged in user name from being displayed.
- Use a non-descript carrying case.
- Be careful when logging online in a wireless hot spot, such as a hotel, café, or airport lounge, as you may not be logging on to a valid wireless network. You may log on to someone nearby with a wireless computer attempting to steal your identity.
- Have your laptop configured to not auto-connect to wireless access points that are listed as "unsecure."
- Regularly check with the manufacturer of your device for news or software updates or any specific security vulnerabilities.

13.0. REFERENCES/BIBLIOGRAPHY

Please note that references and bibliographic information may apply to more than one heading, but are listed only under the first heading to which they apply.

STRATEGIES and MANAGEMENT PRINCIPLES

ASIS International (2005). *Business continuity guideline: A practical approach for emergency preparedness, crisis management, and disaster recovery*. Alexandria, VA: ASIS International. Retrieved on November 29, 2006 from www.asisonline.org/guidelines/guidelines.htm

ASIS International (2004). *Protection of assets manual*. Alexandria, VA: ASIS International.

ASIS International (2006). *Trends in proprietary information loss*. Alexandria, VA: ASIS International.

Doswell, B. & Watson, D. L. (2002). *A guide to information security management*. Leicester, U.K.: Perpetuity Press.

Fennelly, L. J. (Ed.). (2004). *Handbook of loss prevention and crime prevention* (4th ed.). New York, NY: Butterworth-Heinemann.

Heffernan, R.J. (2001). *Developing an information security strategy using a risk based approach* (White Paper). Guilford, CT: R J Heffernan and Associates, Inc.

Thatcher, C. (2006, January). Top security trends for 2006. *CSO Online*, January 2006. Retrieved November 29, 2006, from www.csoonline.com/read/010106/caveat010906.html

BASIC PRINCIPLES

ASIS International (2005). *Information protection toolkit*. Alexandria, VA: ASIS International. Retrieved November 29, 2006 from <http://www.asisonline.org/councils/SPI.xml>

Interagency OPSEC Support Staff (IOSS), www.iooss.gov

OPSEC Professional Society (OPS), www.opsecsociety.org

Office of the National Counterintelligence Executive, www.ncix.gov

NON-TECHNICAL CONTROLS

Awareness of National Security Issues and Response, Federal Bureau of Investigation (FBI), www.fbi.gov/hq/ci/ansir/ansirhome.htm

Information Asset Protection Council, ASIS International, www.asisonline.org/councils/SPI.xml

Longmore-Etheridge, A. (2004). On the eve of destruction," *Security Management*, 48(12), 59-62.

National Association for Information Destruction, Inc., www.naidonline.org

Nolan, J. (1999). *Confidential: Uncover your competitors' top business secrets legally and quickly—and protect your own*. New York, NY: Harper Collins.

TECHNICAL CONTROLS

CERT, Carnegie Mellon University, www.cert.org

Computer Security Institute (2006). *CSI/FBI computer crime and security survey*. San Francisco, CA: Computer Security Institute.

Defense Information Systems Agency (2005, July). *Enclave Security Technical Implementation Guide v3r1*. Retrieved on November 29, 2006, from <http://iase.disa.mil/stigs/stig/enclave-stig-v3r1.pdf>

Heffernan, R.J. (1993). Proprietary information: Technical surveillance countermeasures inspections. In J. Fay (Ed.), *Encyclopedia of security management* (pp.586-588). New York, NY: Butterworth-Heinemann.

National Institute of Standards and Technology (2006). *National vulnerability database*. Retrieved on November 29, 2006 from <http://nvd.nist.gov>

SANS Institute (2006). *SANS top-20 Internet security attack targets*. Bethesda, MD: SANS Institute. Retrieved November 29, 2006, from <http://www.sans.org/top20/?ref=1814>

United States Computer Emergency Readiness Team (2006). *US-CERT vulnerability notes database*. Retrieved on November 29, 2006, from www.kb.cert.org/vuls

United States Department of Justice (2006). *Computer crime and intellectual property section*. Retrieved on November 29, 2006 from <http://www.cybercrime.gov/>

LEGAL CONTROLS

Dorr, R. C. & Munch, C. H. (1999). *Protecting trade secrets, patents, copyrights, and trademarks*, New York, NY: Aspen Publishers.

Garner, B. A. (Ed.) (2004). *Black's law dictionary* (8th Ed.). St. Paul, MN: West Publishing.

United States Patent & Trademark Office, www.uspto.gov

SPECIAL ENVIRONMENTS

Arms Export Control, U.S.C. Title 22, Chap. 39.

Department of State, U.S.C. Title 22, Chap. 38.

International Traffic in Arms Regulations (ITAR), 22 CFR Pts. 120-130.

United States Department of Defense (2006). *National industrial security program operating manual (DoD 5220.22-M)*. Washington, DC: United States Department of Defense.

Retrieved on November 29, 2006, from <http://www.dss.mil/seclib/index.htm>

Bureau of Industry and Security, www.bis.doc.gov

Overseas Security Advisory Council (OSAC), www.osac.gov

14.0. APPENDIX A – SAMPLE POLICY ON INFORMATION ASSET PROTECTION

The following sample policy for Information Asset Protection, a compilation of several real-world corporate policies, can be tailored to any organization. In adapting the policy to your organization, we suggest a review of **Sections 11** and **12** of this guideline to determine if any additional issues need to be addressed in your particular environment.

SAMPLE **ORGANIZATIONAL POLICY ON** **INFORMATION ASSET PROTECTION**

Policy Overview

We are committed to protecting the organization’s assets, including employees, information, and work environment, to enable us to achieve our business goals. As such, we have established this Information Asset Protection (IAP) Policy. It sets forth our guiding principles with respect to protecting the organization’s information assets.

Information is a key organizational asset and will be protected commensurate with its value and based on the results of periodic risk assessments. The protection strategy is based on the following principles:

- Protecting information assets will consist of identifying, valuating, classifying, and labeling in an effort to guard against unauthorized access, use, disclosure, modification, destruction, or denial.
- Controls will represent cost-effective, risk-based measures consistent with other policies and the strategic goals of the organization.
- The IAP strategy integrates traditional security, Information Technology security, legal, and administrative functions.
- Responsibility and accountability extends to all employees as well as the extended enterprise including consultants, contractors, sub-contractors, part-time employees, temporary employees, interns, teaming partners, and associates.
- We will meet all applicable legal and regulatory requirements.

IAP Program Manager

All questions, issues, and concerns related to this policy will be directed to the IAP Program Manager. [Identify the specific contact by name, department, office, or title along with physical location, telephone number, and e-mail. You may also wish to designate a page on your Intranet or Web site for information on this subject.]

Applicability

The IAP policy and principles apply to all employees. It also applies to the “extended enterprise” which consists of both individuals and entities with access to the organization’s information assets, people, and facilities.

Information Assets

Our information assets fall into a variety of categories, some of which are subject to specific laws and regulations. In those cases, we will comply with all applicable laws and regulations. This may become complicated in some circumstances when laws and regulations at the local, state, federal, and international levels may all apply. Contact the organization's Counsel or IAP Program Manager for guidance in specific cases.

The major categories of information assets include: privacy information, proprietary information, trade secrets, patents, copyrights, trademarks, financial data, and regulated information. Each of these categories warrants certain protections according to the IAP policy. More specific guidance is provided in the applicable practices and procedures. [We suggest that you make such procedures and practices available on the organization's Intranet via a Web page for IAP. The page should also identify the IAP Program Manager to whom questions may be addressed.]

Information Classification and Sharing

It is essential to share information both internally and externally in order to perform our mission, leverage innovation, and achieve our business objectives. However, it is also our responsibility to ensure that sensitive information assets are protected from loss or compromise. All employees and members of our extended enterprise are responsible for sharing information assets appropriately and protecting them from inappropriate disclosure, modification, misuse, or loss.

To protect information (paper, electronic, verbal, etc.) according to its business value, we have developed policies, practices, and procedures as part of our IAP Program. This includes a mechanism to classify our most sensitive information assets into four categories: *Highly Restricted*, *Restricted*, *Internal Use*, and *Unrestricted*. Procedures that provide the appropriate level of security control and access to information are based on these classifications:

Highly Restricted is used for proprietary information that could allow a competitor to take action which could seriously damage our competitive position in the marketplace, or the disclosure of which could cause significant damage to the organization's financial or competitive position. Strict precautions are used to eliminate accidental or deliberate disclosure and to detect unauthorized attempted access. Access for employees is limited to specifically named or authorized individuals. Access for non-employees (i.e., our extended enterprise) is limited to individuals who are approved and are covered by a Non-Disclosure Agreement (NDA).

Restricted is used for information that is organizationally or competitively sensitive, or could introduce legal or employee privacy risks. Careful precautions are used to reduce accidental or deliberate disclosure. Access for employees is based on the individual's role. Access for non-employees (i.e., our extended enterprise) is limited to individuals who are approved and are covered by a NDA.

Internal Use is used for information generated within the organization that is not intended for public distribution. Common sense precautions are used to reasonably protect this information. Access is generally limited to employees. Access for non-employees (i.e., our extended enterprise) is limited to individuals or organizations that are approved and are covered by a NDA.

Unrestricted is used for information that can be shared within the organization and outside of the organization.

Each of us is responsible for

- Following all procedures and practices regarding the protection of information assets

- Participating in incident management, risk assessments, work processes, and control mechanisms that support the policy
- Ensuring proper access controls are in place to any information that you create and/or own
- Using common sense and forethought in the release of organization-related information

Employees in designated roles have been assigned specific responsibilities for the deployment, implementation, and maintenance of the IAP policy. These roles and their responsibilities are as follows:

The IAP Program Manager is responsible for overall policy. This may include, but not be limited to:

- Determining the levels and the protection required within each level
- Providing baseline information security through the organization's technology infrastructure
- Providing IAP Management Reports as appropriate
- Coordinating the program with other members within the organization

Management may also designate others within the organization (including the organization's Counsel, Human Resources, Information Technology, Security, etc.) with responsibility for providing direct support, advice, and guidance to the IAP Program. These responsibilities may include assisting in policy, practice, and procedure development, program implementation, program evaluation, investigations, and corrective actions.

Organization Managers and Directors are responsible for employee understanding of and compliance with the IAP policy as well as organizational practices and procedures. This may include, but not be limited to:

- Training employees on all classification levels
- Ensuring policy deployment, work processes, and controls exist within the organization to support the policy
- Ensuring risk assessments are conducted as needed and that incidents are managed within the framework of the IAP policy.

Additional detail on Information Security procedures can be found on the IAP Web Page at _____ . [Insert Intranet reference for your IAP Web page.]

Employee Privacy

Employee data is also an organizational resource, to be protected against alteration, loss, or unauthorized disclosure. We guard information that is essential to running the business and protect this information from disclosure to anyone other than those who have a legitimate business need or legal right to have it.

The privacy and confidentiality of personnel records must be assured. Only that personal information pertinent to decisions made in the course of employment or required for legal purposes is collected. Any personal information collected by the organization will be necessary and relevant, and will be obtained and maintained using methods which respect the individual's right to privacy as well as applicable laws and regulations. In addition, each employee has the right to know what type of personal information the organization maintains about him/her and how it is or may be used.

Periodic audits may be conducted to ensure compliance with organizational policy as well as laws and regulations regarding privacy and personal information management.

Securing Our Property

We are committed to providing security for our tangible and intangible assets to avoid loss.

Each of us:

- Helps to ensure access to the organization's facilities is limited to authorized persons or approved visitors
- Wears and displays appropriate identification as defined by organizational policy
- Addresses security issues in a proactive manner, seeking early involvement and consultation of Security with issues of new brand initiatives, construction projects, etc.
- Takes personal responsibility for being aware of and taking appropriate action on potential security risks in the work environment

Local management:

- Ensures facilities meet recommended access control standards and comply with other security guidance
- Responds to security incidents and/or concerns, ensuring they are properly reported to Security

Security, in conjunction with IT and other appropriate departments within the organization, has the responsibility to conduct any investigative activities in cases of known or suspected information loss, compromise, theft, data manipulation, denial of access, fraud, or conflict of interest. Security also has the responsibility for involving local authorities as appropriate in these investigations. Specialized expertise should be engaged through trusted external providers when appropriate to support security investigations.

Specific measures for handling sensitive information, marking, storage, transmission/transport, copying, declassification, and destruction of sensitive information in all forms are provided in our organization's practices and procedures available on the Intranet at _____ [Insert Intranet reference for your IAP Web page.]

Security Awareness and Training

Each employee and member of the extended enterprise is responsible for protecting our information assets. Each individual must also be aware of the reasons or need for controls, as well as the practices and procedures that comprise our IAP Program. Security, in conjunction with the IAP Program Manager, will provide periodic security awareness training that will include up-to-date information on the risks to information assets and prudent defensive measures. Awareness will also be facilitated through regular newsletter articles, reminders, and Web-based resources.

Our intention is to: a) keep security at the forefront of peoples' minds, and b) give everyone the tools he or she needs to protect information assets. Easy and quick access to the practices and procedures they need – as well as useful answers to their questions – will help ensure that all members of our organization, including our extended enterprise, are involved on a daily basis in protecting our business success.

Public Release of Information

Direct all media inquiries to the External Affairs (or Public Affairs) Director. This action should help ensure that public information remains consistent and monitored.

Publications and Presentations

We encourage the appropriate sharing of information through presentations and publications. Such sharing fosters innovation, networking, market development, public relations, and community awareness.

Any information shared must follow the IAP policy regarding security precautions for each respective classification level. Contact your manager if you have any questions or concerns regarding the information to be shared.

Make the External Affairs (or Public Affairs) Department aware of all planned presentations and publications to outside organizations or groups. Presentations and publications that could potentially involve Restricted or Highly Restricted information should be consistent with the organization's IAP policy.

Travel Security Planning

Information assets are particularly vulnerable during both domestic and international travel by the organization's employees and associates. As such, special precautions are appropriate prior to, during, and following business travel.

Security Awareness training programs that address the security precautions to consider while in travel status should be developed. The security training should review relevant security practices and procedures, discuss the safety and security environment of the particular location(s) involved, and provide for specific security measures, if appropriate. These may include visit requests/notifications, reporting procedures, material packaging or forwarding, preparation of media (e.g., CDs, DVDs, wireless devices, hard drives, etc.) and other issues. Ensure that information and physical property (such as notebook computers and handheld devices) will be adequately protected, and that the traveler is prepared to be safety- and security-conscious. Any security or safety related issue, suspicious activity, or problems encountered should be promptly reported to Security, the IAP Program Manager, or your manager.

Notebook computers and handheld devices are particularly vulnerable to theft during travel, at such places as busy airports, meetings, and conferences. The use of wireless devices and networks outside of the organization's facilities is subject to restrictions outlined in the organization's practices and procedures. In addition, do not discuss sensitive information in public places where conversations can be overheard or recorded – or with individuals who do not have a need-to-know. Be wary of individuals who express a high degree of interest in the organization's projects or information.

New Projects and Initiatives

All new research, development, product line or brand initiatives should be protected using the security principles and strategies detailed in the IAP policy and the supporting practices and procedures. An IAP plan should be considered for any projects involving Highly Restricted or Restricted information.

Information Technology (IT) Resources

Computers, peripherals, handheld, and wireless devices owned and/or issued by the organization remain the property of the organization and are intended for business use only. All such systems and the information contained on them are subject to monitoring or review by the organization's officials or representatives, and no expectation of privacy exists in the possession or use of these systems. Individuals (employees and members of the extended enterprise) are responsible for proper handling and protection of all hardware, firmware, software, data, and information associated with these systems. This includes

ensuring that software is properly licensed and that the equipment is reasonably protected from theft, tampering, and misuse.

In addition, individuals are responsible for protecting any and all information that may reside on such systems, regardless of its sensitivity or subject matter. Information must be properly protected while resident on the system and while being processed, copied, transmitted, received, or exchanged.

Although a limited and reasonable amount of non-business use may be tolerated in some cases (e.g., receiving a personal phone call on a organization-issued mobile telephone), such use should be minimal and proper security measures still apply. When using such systems, comply with all IT, communications, and other relevant policies. Under no circumstances will any inappropriate matter (e.g., pornography, illegal activities, defamatory material, threats, etc.) be accessed, downloaded, stored, transmitted, or processed on organization owned or issued systems.

Web Presence

Ensure that information you post on your organization's Web site is properly protected using the IAP policy procedures for Highly Restricted, Restricted, and Internal Use information. The organization's Web site is accessed and viewed by many individuals and the appropriate level of protection must be implemented. All employees should be aware that information on a topic may appear on several different pages within the Web site itself and should ensure that all pages reflect the same level of information and the ability to access.

Trusted Relationships (Extended Enterprise)

Specific obligations, practices, and procedures for IAP will be documented in written agreements prior to the execution of any contract, consulting engagement, or other business relationship which may involve the exchange of or access to sensitive information. The agreements may include an NDA, contract clauses, memoranda of understanding, and/or other formats. The agreement should specify the type of information to which it applies, the identity of the parties involved, the purpose of the agreement, and the time period for which it will remain valid. Specific reference to the IAP policy and other relevant organizational policies, practices, and procedures will be made in all such agreements.

Individuals and entities in a trusted relationship with our organization should be made aware, consistent with the NDA that is in place with the individual or entity, that their obligation to protect certain information may extend beyond the time period of their relationship with us or the end of the particular project to which the agreement applies. In addition to our written agreement, local, state, federal, and/or international laws and regulations may also apply to information protection and disclosure matters.

Reporting Suspicious Activity or Suspected Loss/Compromises

All inappropriate approaches by individuals (in person or electronically) requesting sensitive information and other suspicious activity should be reported. In addition, any suspected loss or compromise of sensitive information should be reported. Report such incidents to the IAP Program Manager and/or Security via the most expedient means. If relevant to your organization, reporting may also be accomplished through your organization's "Alert Line" at _____. [Insert phone number]

This organization abides by copyright, trademark, trade secret, and patent law.

Employees who violate this policy – either intentionally or through negligence – may be subject to disciplinary action, including possible termination. In addition, employees, individuals, and entities

covered under this policy may be subject to administrative actions, criminal prosecution, and/or civil actions for violations.

15.0. APPENDIX B – QUICK REFERENCE GUIDE

The Quick Reference Guide presented on the following pages is a straightforward and widely applicable tool that every employee or trusted associate of an organization may use to determine the proper classification of material and relevant procedures for handling sensitive information.

The Quick Reference Guide can easily be tailored to any organization and adapted for use by key management decision makers, managers with specific responsibility for information assets protection, or all employees.

QUICK REFERENCE GUIDE for INFORMATION ASSET PROTECTION

This guide has been created as an example of what an organization may create and disseminate to its employees on the use of classifying information and following procedures based on the classification.

**Step
1**

This document is a quick reference guide for information asset owners and users. For more detailed information on specific topics, please see the policy, practices, and procedures manual available at _____. Listed below are the four categories used to classify information and a brief explanation of the procedures to be followed for each classification. All information should be classified under one of the following four categories: Unrestricted, Internal Use, Restricted, or Highly Restricted. Only information under the categories of Internal Use, Restricted, or Highly Restricted is required to be marked. Share or disseminate this information following the procedures listed below for each category. If the information has not yet been classified, proceed to Step 2.

Unrestricted	Internal Use	Restricted	Highly Restricted
<p>This information can be shared within the organization and outside of the organization.</p>	<ol style="list-style-type: none"> 1. Read access is unrestricted within the company. Version control and updates are managed by the content owner. 2. Sharing externally without a non-disclosure requires a clear understanding between the parties that the information is to be treated as confidential. 3. This information is not to be shared with the public. 	<ol style="list-style-type: none"> 1. Content Owners manage access lists and authorize sharing. 2. Access is limited to certain organizations, groups, or people in certain roles (i.e., legal, engineering, marketing, etc.) 3. Breadth and type (e.g. create, read only, update or delete) of Information access is limited and is based on role and fraud control requirements. 4. A signed NDA and an established “need to know” policy are required to share this information with the Extended Enterprise.⁶ 	<ol style="list-style-type: none"> 1. Content Owners manage access lists for type of access and authorized sharing. 2. Access is restricted to specifically named individuals with an established “need to know.” 3. Authorizing a fellow employee requires verification of employee status and a clear understanding of intended use. 4. In authorizing sharing information with an individual from the Extended Enterprise, verify that a signed NDA and an appropriate contractual agreement are in place. 5. Quarterly review of continued access.

⁶ “Extended Enterprise” consists of both individuals and entities with access to the organization’s information assets, people, and facilities.

**Step
2**

Did you create or otherwise own the information?

Yes. I need to determine classification, and I have the authority to classify my information. I will determine the information classification using the following questions. The column with the most selections suggests the protection classification. Caveats:

- Use good business judgment when sharing any business information.
- Share documents in read-only form.

No, but I would like to share it. Share information following the guidance provided in the chart under Step 1. If you have a strong feeling that unmarked information should be marked because it may have a value to competitors or may have proprietary value, contact the information owner to share your concerns. It is the information owner's or creator's responsibility to initially mark and update information classifications.

	Unrestricted	Internal Use	Restricted	Highly Restricted
1. What competitive advantage does this information provide?	None	Possible advantage	Definite advantage	Significant advantage
2. Likelihood that a competitor is seeking this information:	None	Some likelihood	Likelihood exists	Strong likelihood
3. If this information was disclosed, lost, or changed:	None	Some damage	Moderate damage	Severe damage
- Potential damage to organization's operations?				
- Potential damage to an individual?				
- Potential damage to the organization's reputation or image?				
- Loss of customer, shareholder, or business partner confidence?	None	Some chance	Good chance	Definite chance
- Loss of trade secret or patent protection?	None			
- Loss of ability to be first to market?	None			
- Loss of market share?	None			
- Effect on the company's stock value or venture capital support?	None	Little effect	Moderate and short-term effect	Severe and long-term effect
Examples:	Factual information contained in organization's advertising and on its Web sites.	Organization charts, employee directories, maps of the facilities.	Pre-patent data, safety data, product initiative reports, customer data, consumer insights, personnel information, sourcing plans.	Developmental formulas, patent data, consolidated financials, stock actions, global financial system information, flagship brand strategy.

If the information does not meet the minimum criteria for "Internal Use" above, it might be considered public information, unless it falls under a special category such as data restricted by financial, healthcare, or privacy regulations. Check with your IAP Program Manager.

Protection Requirements for Sharing Information Within Various Classifications

Listed below are examples and suggested procedures to follow for the marking and dissemination of documents. Note: International, federal, state, or local laws or regulations may supersede protection requirements. For all electronic systems, the employee must use the organization's owned or approved software, media, and tools.

	Internal Use (Green)	Restricted (Yellow)	Highly Restricted (Red)
Marking			
Documents (Paper and electronic)	Only items with broad corporate circulation are marked "Internal Use" and these are shared in non-editable form.	Mark "Restricted" on the <i>first</i> page or mark at Application/Web site entry.	Mark "Highly Restricted" on <i>every</i> page and every screen that displays or provides access to Highly Restricted data.
Mailing/Shipping			
Within the company	Routing envelope with no special markings.	Double, sealed envelopes. Mark inner envelope "Restricted: to be opened by addressee only." No security marks on outer envelope.	Double, sealed envelopes. Mark inner envelope "Highly Restricted: to be opened by addressee only." No security marks on outer envelope.
Facsimile (FAX)			
Within the company	No special requirements.	Confirm fax number and ask if machine is physically secured. Ask recipient to be present while fax is received.	Avoid Faxing across international borders, if possible. If sent, neutralize or sanitize contents to degree practical.
Over Outside Lines	Notify recipient and confirm the fax number.	Ask that recipient be present while fax is received.	Fax if other more secure methods of transference are unavailable. <ol style="list-style-type: none"> 1. Neutralize /sanitize contents to degree practical. 2. Request recipient to be present during receipt. 3. Do not draw attention to sensitivity by marking cover sheet.
E-mail/Electronic Transfer			
Within the company (intranet, encrypted links, dedicated lines)	No special requirements	Encryption is recommended but not required for internal electronic communications.	<ol style="list-style-type: none"> 1. Encrypt email messages or files, if possible. 2. Use encryption technology, if possible. 3. Validate business need and identity of the receiver.
Through Outside Networks (Internet)	<ol style="list-style-type: none"> 1. Address to specific individuals. 2. Do not post on bulletin boards or send to public forums. 	<ol style="list-style-type: none"> 1. Use encryption technology, if possible. 2. Validate business need and identity of the receiver. 	
Storage			
Within the company	Use password enabled screen saver with timeout less than 15 minutes.	<ol style="list-style-type: none"> 1. Encrypt electronic documents and control access. 2. Maintain personal control or use locked storage. 	
Off company premises	<ol style="list-style-type: none"> 1. Keep Information under your control. 2. Use password enabled screen saver with timeout less than 15 minutes. 		
Destruction/Disposal			
Within the company and offsite	<ol style="list-style-type: none"> 1. Where appropriate, adhere to the organization's retention limits. 2. Shred hard copy or use locked recycle bins. 3. Delete electronic information. 4. Destroy removable media (e.g., diskettes, CD's, tape cartridges, zip disks, etc.) before disposal. 		