

Information Asset Protection

G U I D E L I N E

ASIS INTERNATIONAL COMMISSION ON GUIDELINES

The Commission on Guidelines was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector secure its business and critical infrastructure, whether from natural disaster, accidents, or planned actions, such as terrorist attacks, vandalism, etc. ASIS had previously chosen not to promulgate guidelines and standards, but world events have brought to the forefront the need for a professional security organization to spearhead an initiative to create security advisory provisions. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhancing the professionalism of the industry.

Mission Statement

To advance the practice of security through the development of guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

Goals and Objectives

- Assemble and categorize a database of existing security-related guidelines
- Develop methodology for identifying new guideline development projects
- Involve ASIS Councils, interested members, and other participants to support guideline development
- Identify and establish methodology for development, documentation, and acceptance of guidelines
- Build and sustain alliances with related organizations to benchmark, participate in, and support ASIS guideline development
- Produce national consensus-based guidelines in cooperation with other industries and the Security Industry Standards Council

Functions

- Establish guideline projects
- Determine guidelines for development and assign scope
- Assign participating Council(s), where appropriate
- Approve membership on guideline committees
- Act as a governing body to manage and integrate guidelines from various Councils and security disciplines
- Review and monitor projects and guideline development
- Approve Final Draft Guideline and Final Guideline
- Select guidelines for submission to the Security Industry Standards Council and the American National Standards Institute (ANSI)



INFORMATION ASSET PROTECTION GUIDELINE

SAFETY Act Designation

In April 2005, the U.S. Department of Homeland Security (DHS) awarded ASIS International a Designation for its Guidelines Program under the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technology Act of 2002). This Designation is significant in three ways: (1) it establishes that ASIS guidelines are qualified to be a “technology” that could reduce the risks or effects of terrorism, (2) it limits ASIS’ liability for acts arising out of the use of the guidelines in connection with an act of terrorism, and (3) it precludes claims of third party damages against organizations using the guidelines as a means to prevent or limit the scope of terrorist acts.

ASIS GDL IAP 05 2007

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. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgment of ASIS International as the source. However, this document may not be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise used commercially.

Copyright © 2007 by ASIS International

ISBN 978-1-887056-70-0

10 9 8 7 6 5 4 3 2 1

ASIS GDL IAP 05 2007

 **Documents**
Document Sharing Hub



Information Asset Protection (IAP) Guideline

1.0	Title	5
2.0	Revision History	5
3.0	Commission Members	5
4.0	Committee Members	5
5.0	Guideline 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 (IAP) 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	13
12.4	Labeling Information Assets	13
12.5	Need-to-Know Controls	13
12.6	Privacy Protection	13
12.7	Information Security Awareness and Training	14
12.8	Key Projects and Other Potentially Competitive Information	14
12.9	Investigating Loss or Compromise	15
12.9.1	Investigation	15
12.9.2	Damage Assessment	15
12.9.3	Root Cause Analysis	15
12.10	Handling, Receipt, Transmission, Storage, and Destruction	16
12.11	Protection of Information in Hard Form (Physical Product)	17
12.11.1	Prototypes and Models	17
12.11.2	Manufacturing Processes and Equipment	17
12.11.3	Compartmentalization and Physical/Visual Barriers	18
12.11.4	Preventing and Detecting Counterfeiting and Illegal Copying	18
12.12	Technical Security Controls	18
12.13	Technical Surveillance Countermeasures (TSCM)	19
12.14	Information Systems Security	19
12.15	Network Intrusion Detection and Extrusion Prevention Systems	20
12.16	Firewalls	20

12.17	Logical Network Access Control	20
12.18	Application Security	20
12.19	Sanitizing Information Systems and Media	21
12.20	Data Security	21
12.20.1	Encryption	21
12.20.2	Digital Signatures	21
12.21	The Wireless Environment	21
12.22	Legal Protections	21
12.22.1	Trade Secrets	22
12.22.2	Patents	22
12.22.3	Copyrights	22
12.22.4	Trademarks and Service Marks	23
12.23	Agreements Protecting Information	23
12.24	Protecting Information in Special Environments	23
12.24.1	Telecommuting and Remote Access	23
12.24.2	E-Conferencing	24
12.24.3	Domestic and International Travel	24
12.24.4	Trade Shows	25
12.24.5	On- and Off-Site Meetings	25
12.25	Outsourcing to Providers	26
12.25.1	Contractor and Subcontractor Relationships	27
12.26	Cell Phones, Laptops, and PDAs	28
13.0	References/Bibliography	29
14.0	Appendix A - Sample Policy on Information Asset Protection	32
15.0	Appendix B - Quick Reference Guide	39

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, Northwest Airlines

5.0 GUIDELINE DESIGNATION

This guideline is designated as ASIS GDL IAP 05 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 valuated, 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 Security: Measures taken to identify, prevent or neutralize technical threats including electronic or electro-optic eavesdropping, wiretapping, bugging, signal intercept, covert/illicit surveillance, and attacks on Information Technology (IT) or telecommunications systems.

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

Any successful program is based on a clear, practical and communicated policy. To ensure effective implementation, it is essential, at the outset of discussions regarding the Information Asset Protection (IAP) policy, that:

1. An organization's leadership provides 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 Information¹, 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.

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

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 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.

Additionally, the IAP policy should complement or incorporate (as appropriate) information systems considerations such as authorized use policies or acceptable use policies for information and telecommunications systems (see Section 12.14).

The protection of information assets should be incorporated into the organization's Business Continuity Plans to ensure that critical information retains its availability, confidentiality and integrity during all phases of crisis situations including response and recovery. Plans should be communicated to all appropriate personnel and exercised on a periodic basis. (For further information, see the ASIS Business Continuity Guideline, available on the ASIS Web Site at www.asisonline.org/guidelines/guidelines.htm.)

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?
- What is the effect on national security or government security?

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 conduct of appropriate IPR risk assessments as part of a due diligence process prior to any business transaction. Risk analyses can be performed on a qualitative or quantitative basis. Too often there is an over-emphasis on dollar values as the only metric. This may discourage the consideration of non-tangible measures or factors, which cannot be easily quantified. For this reason, qualitative risk analyses are sometimes more appropriate and should be considered in lieu of or in addition to quantitative analyses.

Assessments must also be performed at the proper "level" in an enterprise. They need to be considered at the product, technology, *and* transaction-specific level in order to be most effective at identifying and addressing risk.

Additional information on conducting certain types of risk assessments is available in the ASIS General Security Risk Assessment Guideline at www.asisonline.org/guidelines/guidelines.htm.

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 and customer privacy is not compromised.
- Provide a mechanism to investigate compromises of privacy information (including identity theft) and report the incidents to affected individuals or organizations (victims) as appropriate.