

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 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

10987654321

ASIS GDL IAP 05 2007



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.

If You Would Like to View the Complete Article,
Become a Member of ICOR. It's easy and you'll have
access to this and other informative and valuable
presentations and articles.



THE ICOR
The International Consortium For Organizational Resilience

www.theicor.org