

Privacy Fundamentals: What an Information Security Officer Needs to Know

Author: Bruce J. Bakis,

Contributors: Richard D. Graubart,
Julie S. McEwen, Stuart S. Shapiro

October 18, 2005

Content

- **Scope**
- **The basics of privacy**
- **Privacy challenges**
- **Security vs. Privacy**
- **A winning privacy strategy**
- **Overview of the legal and regulatory privacy landscape**
- **Privacy risk assessment and management**
- **Model Privacy Program**
- **Privacy principles and practices**
- **Common security-related privacy problems**
- **Summary**

Scope

■ This session is not ...

- An academic treatise on privacy
- A comprehensive overview of privacy laws and regulations
- Implementation guidance for compliance with privacy laws and regulations
- Focused on rights of employees to privacy
- An overview of what Information Privacy Officers or Managers should know and do

■ This session is ...

- Focused on the basics of what an Information Security Officer or Manager should know and do about privacy
- Focused on information privacy

The Basics of Privacy

Key Definitions

Information Privacy

- **Individual:** The right of an individual to exercise control over the collection, use, and dissemination of his or her personal information
- **Organization:** The right to appropriately use personal information

Personal Information

- Any information collected or maintained about an individual, other than items of public record, that identifies or can be used to identify, contact or locate him or her.
- Confidentiality must be maintained

Confidentiality

- Assurance that personal information is not disclosed to unauthorized entities (people and systems)

Major Privacy Dimensions

Bodily Integrity

- Maintaining integrity of an individual's body (e.g., blood, DNA sampling)

Behavior

- Maintaining privacy of personal activities (e.g., political activities, religious practices)

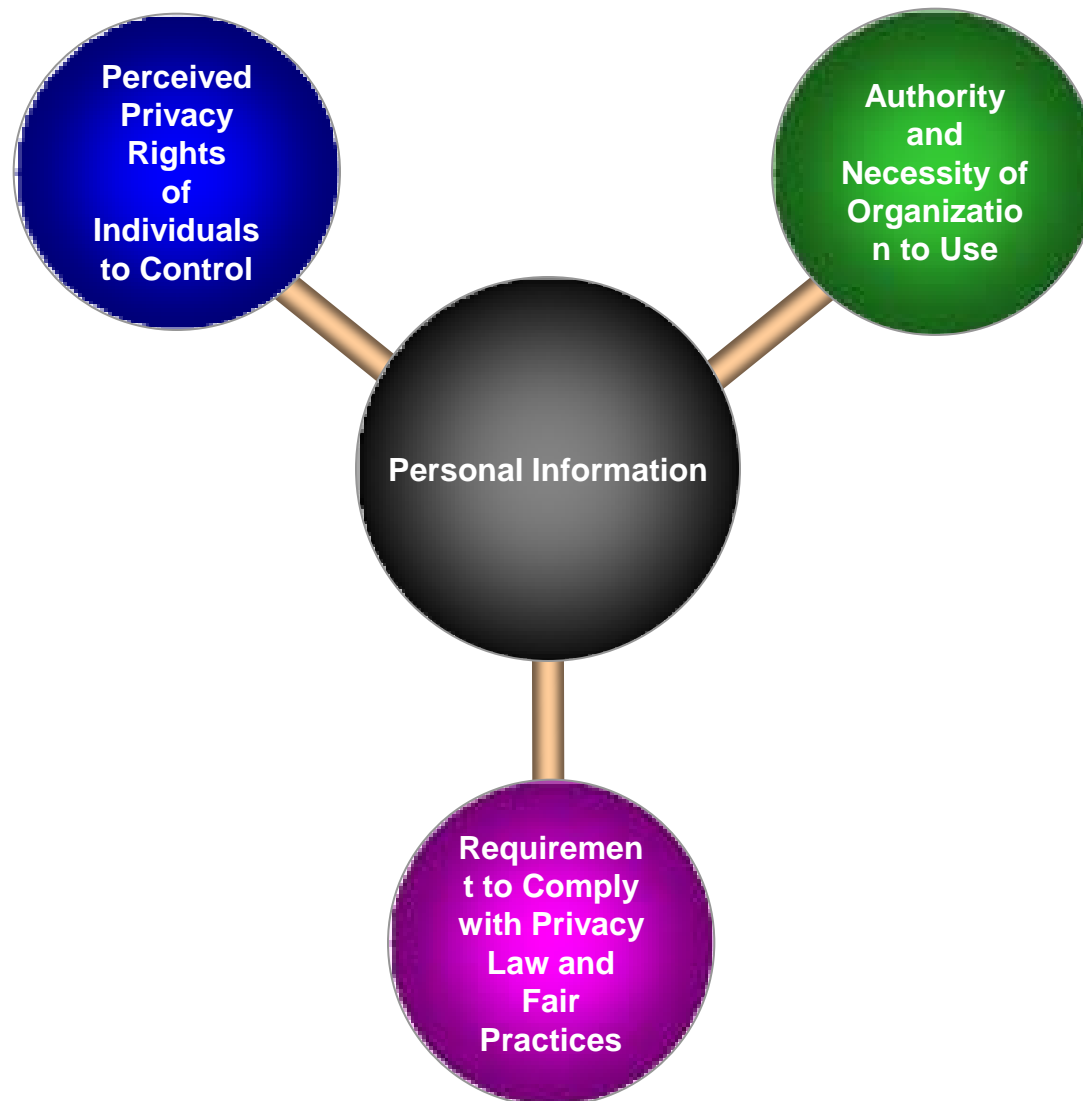
Communications

- Communicating without undue monitoring (e.g., phone calls, e-mail)

Information

- Determining when, how, and to what extent an individual will share information about himself or herself (e.g., home telephone)

The Privacy Challenge (1 of 2)



The Privacy Challenge (2 of 2)

Privacy issues and risks exist in a complex context

- **Need Privacy Systems Engineering approach: a repeatable, scalable, systems engineering-based approach to uncovering, understanding, and addressing privacy issues and risks**
 - Explicitly considers a multi-dimensional context as well as technology
 - Uses risk management to minimize unintended consequences
 - Aligns privacy solutions with mission requirements



Security vs. Privacy (1 of 2)

- You can have good security without privacy, as long as there's no personal information involved
- But you can't have good privacy without security

Privacy: focuses on individual's ability to control Personal Information


- Business Continuity
- Protecting both system and information from threats
 - Application and System Security in Development
 - Security Architecture
 - Configuration and Patch Management
 - Intrusion Detection and Mitigation
- Physical protection

- Accountability
- Integrity
- Aggregation
- Confidentiality
- Destruction

- Identifying uses and users of PI
- Seeking agreement to use of PI
- Being open, honest and respectful
- Limiting PI collection
- Limiting use of PI to identified purposes
- Providing avenues for complaints
- Allowing access to PI to maintain accuracy and completeness

Information Security: focuses on mechanisms for protecting information and information systems

Security vs. Privacy (2 of 2)



	Security	Privacy
Accountability	<ul style="list-style-type: none"> Focuses on tracking an individual's actions and manipulation of information 	<ul style="list-style-type: none"> Focuses on tracking the trail of PI disclosure
Integrity	<ul style="list-style-type: none"> Protects against the corruption of data by authorized or unauthorized individuals 	<ul style="list-style-type: none"> Seeks to ensure that inaccurate PI is not used to make an inappropriate decision about a person
Aggregation	<ul style="list-style-type: none"> Focuses on determining the sensitivity of derived and aggregated data so that appropriate access guidance can be defined 	<ul style="list-style-type: none"> Dictates that aggregation or derivation of new PI should not be allowed if the new information is neither authorized by law nor necessary to fulfill a stated purpose
Confidentiality	<ul style="list-style-type: none"> Focuses on processes and mechanisms (e.g. authenticators) that prevent unauthorized access 	<ul style="list-style-type: none"> Focuses on ensuring that PI is only disclosed for a purpose consistent with the reason it was collected
Destruction	<ul style="list-style-type: none"> Focuses on ensuring the information cannot be recovered once deleted 	<ul style="list-style-type: none"> Addresses the need for the complete elimination of collected information once it has served its purpose

A Winning Privacy Strategy

- **Establish a high standard of privacy protection to:**
 - Facilitate necessary and appropriate cross-boundary sharing of personal information in support of the organization's mission
 - Comply with the letter and the spirit of privacy laws and regulations
 - Build trust and respect among constituents
 - Reduce threats to personal information, especially identity theft and insider threat
- **Respect the privacy rights and expectations of individuals while achieving the organization's mission**
- **Use Privacy Systems Engineering to assess and manage risk**

Legal and Regulatory Landscape (1 of 2)

Key U.S. Privacy Legislation

- Fair Credit Reporting Act (1970)
- Privacy Act (1974)
- Freedom of Information Act (FOIA) (1974)
- Family Educational Rights and Privacy Act (1974)
- Right to Financial Privacy Act (1978)
- Electronic Communications Privacy Act (1986)
- Computer Matching and Privacy Protection Act (1988)
- Video Privacy Protection Act (1988)
- Employee Polygraph Protection Act (1988)
- Driver's Privacy Protection Act (1994)
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Children's Online Privacy Protection Act (COPPA) (1999)
- Financial Modernization Services Act/Gramm-Leach-Bliley (1999)
- USA PATRIOT Act (2001) (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorists)
- Data Quality Act (2002)
- **E-Government Act (2002)**

Key Office of Management and Budget (OMB) Privacy Guidance

- OMB M-99-18, Privacy Policies on Federal Web Sites
- OMB M-00-13, Privacy Policies and Data Collection on Federal Web Sites
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal privacy
- **OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002**
- OMB M-04-26, Personal Use Policies and “File Sharing” Technology
- OMB M-05-04, Policies for Federal Agency Websites
- **OMB M-05-08, Designation of Senior Agency Officials for Privacy**
- **OMB M-05-15, FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management**

Legal and Regulatory Landscape (2 of 2)

OMB Guidance for Designation of Senior Agency Officials for Privacy (February 11, 2005)

- Each federal agency needs to identify to OMB the senior official with agency wide responsibility for information privacy

OMB FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (June 13, 2005)

- Federal agencies must report on effectiveness of privacy program in annual FISMA report (October 7, 2005)

OMB Guidance for Implementing E-Government Act (September 26, 2003)

- Provides requirements for federal agencies to conduct Privacy Impact Assessments (PIAs)

Risk Assessment and Management (1 of 2)

Privacy Impact Assessment (PIA)

What	<ul style="list-style-type: none">• A PIA is a document of an assessment of actual or potential impacts—including social and ethical—that a federal system may have on privacy and the ways in which any adverse impacts may be mitigated
Requirement	<ul style="list-style-type: none">• Section 208—Privacy Provisions—of the E-Government Act requires all federal agencies to complete PIAs for new or substantially modified information systems that handle personal information• <i>Although it's a requirement for federal systems, a PIA is an effective privacy risk assessment and management tool for all organizations</i>
OMB Guidance	<ul style="list-style-type: none">• <u>What</u> information is to be collected• <u>Why</u> the information is being collected• Intended <u>use</u> of the information• With whom the information will be <u>shared</u>• What opportunities individuals have to decline to provide information or <u>consent</u> to particular uses of the information• How the information will be <u>secured</u>• Whether a system of records is being created under the Privacy Act• <u>Analysis of choices</u> an agency made regarding an IT system or collection of information• Information lifecycle analysis

Risk Assessment and Management (2 of 2)

PIA vs. Certification and Accreditation (C&A)

Commonalities	
<ul style="list-style-type: none">• Risk-based analysis• Identifies potential risks and mitigation measures• Living entity, updated as system or environment changes	
PIA	C&A
<ul style="list-style-type: none">• Information focused• Assessment report targeted to general public• Periodic reassessment<ul style="list-style-type: none">– Not required if no significant change to system or environment• Validation<ul style="list-style-type: none">– Employs multi-party document review and CPO signoff• Authorization to operate<ul style="list-style-type: none">– No accreditation equivalent• Minimize information flow<ul style="list-style-type: none">– Users/systems only receive information they need	<ul style="list-style-type: none">• Information system focused• Certification report targeted to accreditor• Periodic recertification<ul style="list-style-type: none">– Required every 3 years (even if no change to system or environment)• Validation<ul style="list-style-type: none">– Employs document review, testing, and interviews• Authorization to operate<ul style="list-style-type: none">– Accreditation: go/no go decision• Minimize system access and user privileges

Context for Discussion of Privacy Responsibilities and Practices (1 of 2)

- Need to simplify and normalize privacy requirements

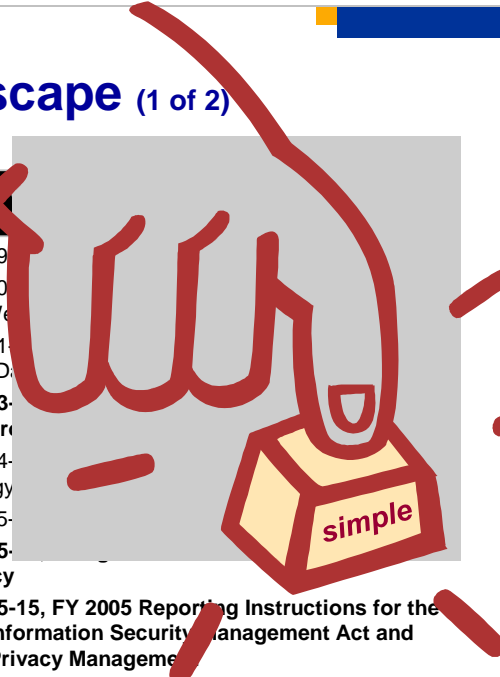
Legal and Regulatory Landscape (1 of 2)

Key U.S. Privacy Legislation

- Fair Credit Reporting Act (1970)
- Privacy Act (1974)
- Freedom of Information Act (FOIA) (1974)
- Family Educational Rights and Privacy Act (1974)
- Right to Financial Privacy Act (1978)
- Electronic Communications Privacy Act (1986)
- Computer Matching and Privacy Protection Act (1988)
- Video Privacy Protection Act (1988)
- Employee Polygraph Protection Act (1988)
- Driver's Privacy Protection Act (1994)
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Children's Online Privacy Protection Act (COPPA) (1999)
- Financial Modernization Services Act/Gramm-Leach-Bliley (1999)
- USA PATRIOT Act (2001) (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorists)
- Data Quality Act (2002)
- E-Government Act (2002)

Key OMB Privacy Policy

- OMB M-99-06, Federal Information Security Management Act
- OMB M-00-04, Federal Information Security Management Act
- OMB M-01-04, Personal Data Privacy and Security
- **OMB M-03-05, Privacy Protection**
- OMB M-04-04, Technology and Privacy
- OMB M-05-04, Privacy Protection
- **OMB M-05-04, for Privacy**
- **OMB M-05-15, FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management**



Model Privacy Program

Privacy Principles

Context for Discussion of Privacy Responsibilities and Practices (2 of 2)

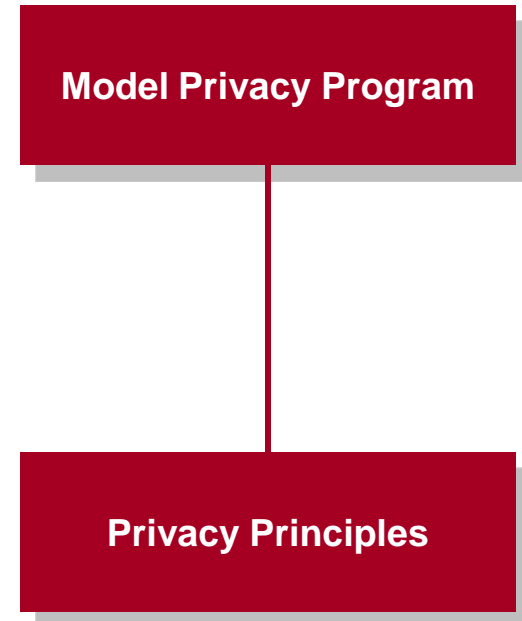
■ Model Privacy Program

- Essential building blocks in an effective privacy program
- Similar to elements in a comprehensive information security program (ISO 17799)

■ Privacy Principles

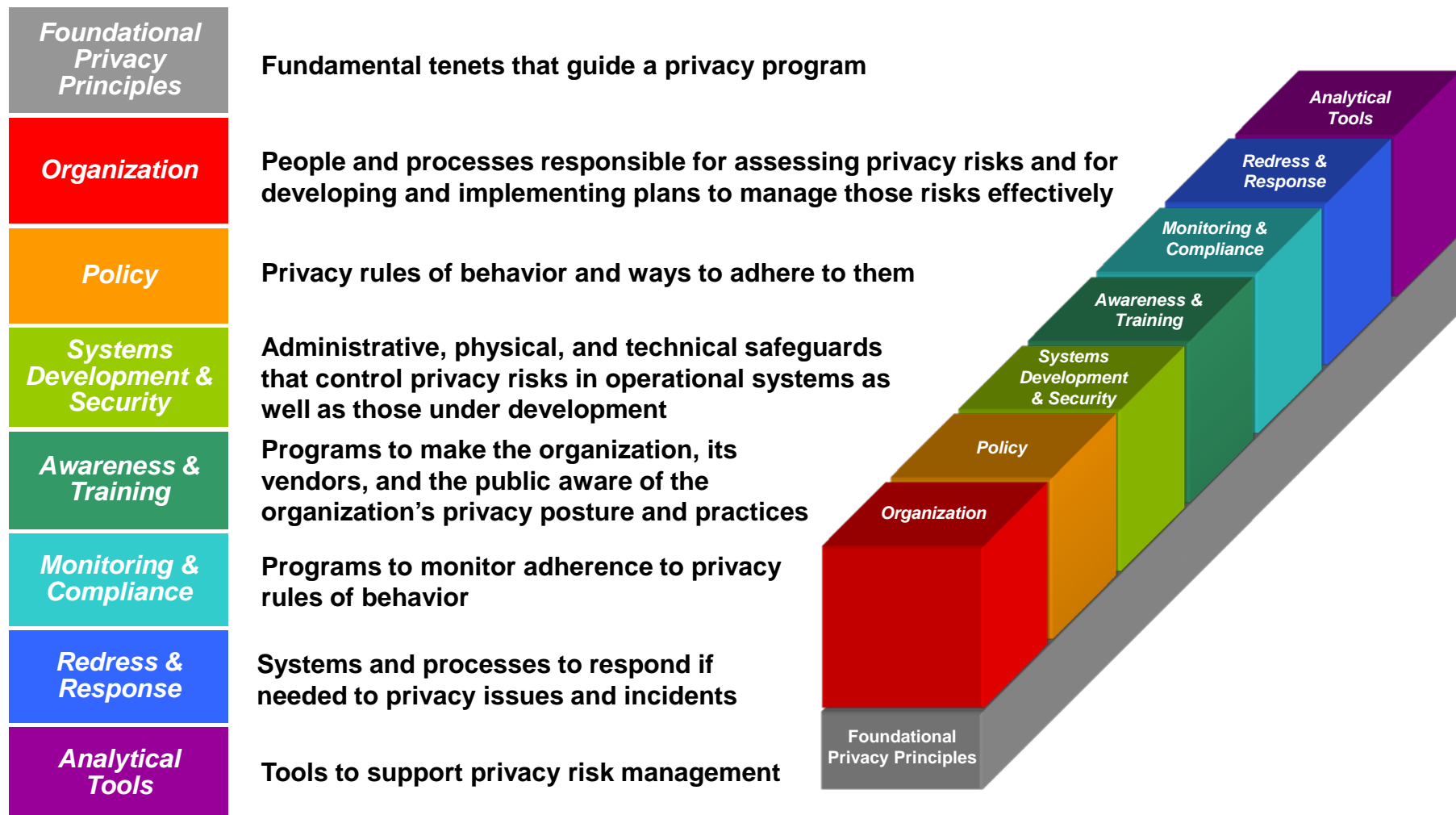
- Tenets for all to adhere to
- Decomposed here into responsibilities, policies and practices for the role of an Information Security Officer/Manager
- There are role-based decompositions for Privacy Officers and for other constituents (e.g., System Manager, Manager, Developer, etc.), but not in this presentation

- Together, they simplify and normalize privacy requirements to a set of essential practices



Model Privacy Program

Essential elements in an effective program



Security Officer Activities (1 of 2)

Element	Description	Security Officer Activities
<i>Foundational Privacy Principles</i>	Fundamental tenets that guide a privacy program	<ul style="list-style-type: none"> • Approves • Enforces • Supports • Tailors for security organization
Organization	People and processes responsible for assessing privacy risks and for developing and implementing plans to manage those risks effectively	<ul style="list-style-type: none"> • Coordinates roles and responsibilities with Privacy Officer • Maintains effective organizational interaction with Privacy Office
<i>Policy</i>	Privacy rules of behavior and ways to adhere to them	<ul style="list-style-type: none"> • Defines/enforces sensitivity levels of personal information • Aligns protection with sensitivity level
<i>Systems Development & Security</i>	Administrative, physical, and technical safeguards that control privacy risks in operational systems as well as those under development	<ul style="list-style-type: none"> • Applies policy to appropriately protect personal information against loss or theft as well as unauthorized access, disclosure, modification, compromise or destruction • Aligns security requirements with privacy requirements for systems • Collaborates with Privacy Officer to conduct privacy risk assessments and manage privacy risks • Collaborates with Privacy Officer to control risks of sharing personal information with 3rd parties

Security Officer Activities (2 of 2)

Area	Description	Security Officer Activities
Awareness & Training	Programs to make the organization, its vendors, and the public aware of the organization's privacy posture and practices	<ul style="list-style-type: none"> Includes security requirements in all privacy awareness and training materials Requires security personnel handling personal information to receive privacy training
Monitoring & Compliance	Programs to monitor adherence to privacy rules of behavior	<ul style="list-style-type: none"> Monitors (audits) and assesses compliance with privacy requirements to prevent: unauthorized access, disclosure, modification, compromise or destruction Collaborates and coordinates with Privacy Officer to report on privacy compliance and remediation planning for security reporting requirements (e.g., FISMA) Coordinates and collaborates with Privacy Officer to track disclosures of personal information to 3rd parties
Redress & Response	Systems and processes to respond if needed to privacy issues and incidents	<ul style="list-style-type: none"> Coordinates privacy incident response capability and plan with Privacy Officer
Analytical Tools	Tools to support privacy risk management	<ul style="list-style-type: none"> Collaborates with Privacy Officer to adapt security risk assessment tools and techniques to privacy risk assessment

Sample Summary Privacy Principles*

1. Responsibility and Accountability	All personnel are responsible and accountable for treating personal information in accordance with these principles
2. Privacy Awareness and Training	All personnel will be trained to properly handle personal information
3. Openness and Redress	The organization will make its privacy policy and practices available to individuals and provide a complaint and redress process
4. Limiting Collection	The collection of personal information will be limited to that which is necessary for identified purposes.
5. Identifying Purpose	The purposes for which personal information is collected will be identified at or before the time of collection
6. Informed Consent	Individuals will be informed of the purposes, uses and disclosures of their personal information
7. Limiting Disclosure and Use	Personal information will be disclosed only to authorized individuals with a need to know and only for uses that are consistent with identified purposes
8. Data Integrity and Fairness	The organization will maintain the accuracy, completeness, and currency of personal information at levels necessary to achieve identified purposes and make fair determinations about an individual
9. Individual Access	Individuals will be provided access to their personal information and have it corrected if permissible and necessary
10. Limiting Retention	Personal information will be retained only as long as is necessary to fulfill identified purposes
11. Security	Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information
12. Respect	Personal information will be treated with respect

* Based on Canadian Standards Association, Model Code for the Protection of Personal Information:
<http://www.privacyexchange.org/buscodes/standard/canadianstandards.html>

Principles, Policies and Practices (1 of 6)

1. Responsibility and Accountability

All personnel are responsible and accountable for treating personal information in accordance with these principles

- The Security Officer is responsible and accountable for compliance with the security provisions of these principles, policies and practices and applicable privacy laws and regulations.
- Protect and manage personal information appropriate to its level of sensitivity.
- Share expertise, experience and perspectives on development and effectiveness of an information protection program: the things that you're done are highly applicable in the privacy domain.
- Coordinate with the Privacy Officer on roles, responsibilities and organizational interactions for safeguarding personal information.
 - Collaborate on risk management, including Privacy Impact Assessment (PIA) and other forms of periodic privacy risk assessment.
 - Jointly develop privacy incident plans and responses.
 - Develop an accountability process for personal information flows across boundaries of organization.

Key:

Principle name

Principle definition

Policies and practices for Information Security Officers/Managers

Principles, Policies and Practices (2 of 6)

2. Privacy Awareness and Training

All personnel will be trained to properly handle personal information

- Collaborate with the Privacy Officer to develop a complementary privacy and security awareness training and communications program.
- Develop a security-specific role-based supplement of privacy training.
- Make sure that all security personnel take privacy training, especially those with access to personal information or involved in forensic investigations of breaches to the confidentiality of personal information maintain by the organization.

3. Openness and Redress

The organization will make its privacy policy and practices available to individuals and provide a complaint and redress process

- Approve the security provisions in the organization's public Privacy Policy/Statement.
- Coordinate with the Privacy Officer on any responses and communications to affected individuals of any material breaches to the security of their personal information.
- Coordinate with Privacy Officer on any external complaints about the handling or management of personal information.

4. Limiting Collection

The collection of personal information will be limited to that which is necessary for identified purposes

- Know what personal information is being collected, categorize it according its sensitivity and apply the appropriate safeguards.
- Raise a red flag if you believe that the collection of personal information has not been minimized enough (the more there is, the more you need to protect).

Principles, Policies and Practices (3 of 6)

5. Identifying Purpose

The purposes for which personal information is collected will be identified at or before the time of collection

- If personal information will be used to test information security safeguards, identify this as one of the intended purposes even if the information is going to be anonymized.

6. Informed Consent

Individuals will be informed of the purposes, uses and disclosures of their personal information

- The organization obtains the informed consent of an individual to collect, use, or disclosure their personal information, except where inappropriate (e.g., national security, law enforcement).
- At a minimum, the organization gains implied consent, i.e., consent that can be reasonably determined through actions or inactions of an individual (e.g., filling in an insurance claim form).

Principles, Policies and Practices (4 of 6)

7. Limiting Disclosure and Use

Personal information will be disclosed only to authorized individuals with a need to know and only for uses that are consistent with identified purposes

- Reinforce the need to maintain strict confidentiality of personal information and minimize disclosure unless there is a need to know.
- Sharing personal information:
 - Make sure that the third party provides a level of information security and privacy protection that is appropriate to the sensitivity level of personal information and that they have a Non-Disclosure Agreement.
 - Make sure that information security and privacy protection standards are included in a Memorandum of Understanding (MOU) and Interconnection Security Agreement.
 - Make sure that a record is kept of personal information disclosures between the organizations.

8. Data Integrity and Fairness

The organization will maintain the accuracy, completeness, and currency of personal information at levels necessary to achieve identified purposes and make fair determinations about an individual

- Maintain a log of changes to personal information.
- Transmit amended information to third parties with whom personal information has been shared.

9. Individual Access

Individuals will be provided access to their personal information and have it corrected if permissible and necessary

- Appropriately authenticate each individual who is making a request.

Principles, Policies and Practices (5 of 6)

10. Limiting Retention

Personal information will be retained only as long as is necessary to fulfill identified purposes

- Retain personal information for only as long as needed to fulfill an authorized purpose.
- Exercise care in the disposal or destruction of personal data to prevent unauthorized parties from gaining access to it.

11. Security

Personal information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information

- Reach an agreement with the Privacy Officer on the levels of sensitivity of personal information that the organization collects and maintains.
- Appropriately protect personal information against loss or theft as well as unauthorized access, disclosure, modification, compromise or destruction.
- Make sure that all employees know how to handle personal information throughout its entire lifecycle.
- Collaborate with the Privacy Officer to periodically conduct assessments to identify privacy risks and determine the appropriate security protections.
- Coordinate with the Privacy Officer on reporting requirements with respect to the protection of personal information and remediation planning to address protection deficiencies.
- Inform affected individuals of any material breach to the security of sensitive or protected personal information (e.g., SSN).

Principles, Policies and Practices (6 of 6)

12. Respect

Personal information will be treated with respect

- **Manage personal information in a respectful manner appropriate to the sensitivity of the information and the context of its use.**
- **Reinforce the need for strict need to know and confidentiality of person information.**
- **Make sure no one in the security organization recreationally browses personal information.**

Common Security-Related Privacy Problems to Avoid

- **Low awareness among personnel of sensitivity of personal information and required safeguards**
 - Leaving personal information unattended on a printer or fax
 - E-mailing personal information without necessary forewarnings or protections
 - Recreational browsing of personal information
 - Improperly disposing of personal information
 - Improperly securing personal information when left unattended
- **Not controlling and tracking sharing of personal information**
- **Inadequate interaction, coordination and collaboration between security and privacy**
 - Assuming that information security controls and measures have addressed privacy concerns and risks
 - Believing that C&A activities subsume PIA requirements

Summary

- **Information Security Officers/Managers need to work in close collaboration with Privacy Officers/Managers to:**
 - Establish a high level of privacy protection
 - Assess and effectively manage risks
 - Maintain statutory, regulatory and organizational compliance with privacy requirements
 - Establish trust and respect
 - Balance rights and expectations of individuals with the need to meet mission and objectives of the organization
- **Key approaches:**
 - Employ Privacy Systems Engineering to analyze privacy in a multi-dimensional context
 - Use Model Privacy Program and Privacy Principles to guide development and gauge effectiveness of privacy practices

System-of-systems
integration and
interoperability

Technical
requirements
and specifications

Source selection
and acquisition
management

Test planning
and evaluation

The MITRE logo is centered on the slide, overlaid on a grayscale image of the Earth. The logo consists of the word "MITRE" in a large, bold, white, sans-serif font. The background of the slide is a solid blue color. Faint, diagonal text in the background reads "SYSTEMS ENGINEERING" and "INFORMATION TECHNOLOGY".

MITRE

Analysis

System Research
and Development

Field integration
planning and support

System architecture

Supportability
and sustainment