Data Security Policy - Structure and Guidelines

By Joel Weise - SunPS℠ Global Security Practice and Charles R. Martin - SunPS Java™ Centers

Sun BluePrints™ OnLine - December 2001

http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-4175-01
Revision 01, 12/18/01
Edition: December 2001

Data Security Policy - Structure and Guidelines

This template provides a brief description of recommended security policy topics and an overview of core security policies. In addition, this template provides a sample Data Security Policy and Statement with commentary explaining the details of each security topic and why it was chosen. Finally, this template provides a detailed list of Security Policy principles. The purpose of this template is to help guide the development and implementation of an industry best practice Data Security Policy.

This template is built on the recommendations made in the Sun BluePrints article, *Developing a Security Policy* (12/01), by Joel Weise and Charles R. Martin. The article is available from:

```
http://sun.com/blueprints/1201/secpolicy.pdf
```

Security Policy Topics

This section provides a brief description of recommended topics for a data security policy.

Statement of Purpose

Why the policy is needed.

Scope

What is the policy's applicability, who and what is covered by it?

Policy Statement

What are the specifics of the policy?

Responsibilities

Who must do what?

Audience

To whom is the policy oriented?

Enforcement

Who is charged with enforcement of the policy?

What are the penalties for non-compliance?

Exception

Describe these and the conditions under which they apply.

Other Considerations

Are there other ancillary considerations that should be stated?

Communicating Policy

Who is responsible for this effort?

What is the process for disseminating the policy?

Review and Update Process

Who is responsible for the update effort?

What is the process?

Under what conditions is the policy reviewed? (for example, annually or only if a problem occurs)

Implementing the Policy

Who is responsible for the implementation effort?

How is it accomplished?

Monitoring compliance

How is monitoring accomplished?

Overview of Security Policies

The following is a list of standard common core security policies.

1. Data ownership, classification, and security
2. Trans-border data flow
3. Data and resource access
4. Password usage
5. Utilization of cryptography and key management
6. Data content
7. Network security
8. Physical security
9. Electronic mail ownership
10. Security incident reporting process
11. Security incident response process
12. Periodic monitoring and audit for policy compliance
13. Firewall implementation and management
14. Virus prevention and protection
15. System and network ownership and management
16. End user accountability and acceptable use
    a. Identification and authentication

17. Records retention and backup
18. Security Awareness and education
19. Partner and 3rd party connectivity
20. System development and deployment
21. System, application, and configuration management
    a. Assurance
    b. Patch management
22. Infrastructure security
    a. Intrusion detection
    b. System hardening

Sample Data Security Policy

The best way to illustrate how to develop and write a security policy is to dissect a sample of one. The following section offers a sample Data Security Policy. Commentary has been added so that one can see why specific topics are included, their content, verbiage, and context.

Introduction

A purpose should be stated in the introduction section. This should provide the reader with an overview of what this policy will state and why it is needed.

The purpose of this document is to define the <COMPANY> Data Security Policy. Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today's environment because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems creates a unique vulnerability for our organization.

Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate

business contracts, trade secrets, and customer privacy; or reduce credibility and reputation with its customers, shareholders and partners. This policy therefore discusses:

- Data content
- Data classification
- Data ownership
- Data security

The introduction also includes an objective statement. For data security, a life cycle methodology is used.

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all of our and all customer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our agents.

A condensation of the overall policy is provided here. The security stance for your organization should be clearly defined here.

This policy defines the <COMPANY> overall security and risk control objectives that we endorse. The premise for the policy can be stated as:

> "Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorized entities."

This embodies the principle of least privilege.

This document forms part of your conditions of employment for employees, a part of the contractual agreement for vendors, suppliers, and third party processor or agents, hereafter referred to as vendors. All parties must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Breach of Policy and Enforcement

What is considered a breach and the consequences of a breach occurring are stated in this section. The breach of a policy usually implies an adverse action. If there are no adverse ramifications of a breach, then you should review the necessity of the policy.

A breach of this policy could have severe consequences to <COMPANY>, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of <COMPANY> senior management. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of a <COMPANY> vendor, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Scope of the Policy

The scope should explain the policy's applicability—that is, who and what are covered by it. The applicability of the policy should be defined by management. The level of definition is dependent upon the intentions of management.

This policy applies to all <COMPANY> and customer data assets that exist in any <COMPANY> processing environment, on any media during any part if its life cycle. The following entities or users are covered by this policy:

- Full or part-time employees of <COMPANY> who have access to <COMPANY> or customer data.
- <COMPANY> vendors or processors who have access to <COMPANY> or customer data.
- Other persons, entities, or organizations that have access to <COMPANY> or customer data.

Data Life Cycle

It is recommended that a data security policy utilize a data lifecycle methodology. This allows for an easier implementation of the policy for different data under different circumstances.

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Usage

Data usage describes how data is utilized. This section should not be overly detailed but rather ensure the consistency of the application of the policy.

All users that access <COMPANY> or customer data for use must do so only in conformance to this policy. Uniquely identified, authenticated and authorized users must only access data.

Each user must ensure that <COMPANY> data assets under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Transmission

Data transmission describes how data is conveyed through a network. As with usage, this should not be overly detailed. Data transmission policy may include the need for the use of cryptography if applicable.

All users that access <COMPANY> or customer data to enable its transmission must do so only in conformance to this policy.

Where necessary, data transmitted must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the <COMPANY> policy on the use of cryptography.

Data Storage

Data storage describes how data is stored or filed. As with usage, this should not be overly detailed. Data storage policy may also include the need for the use of cryptography if applicable.

All users that are responsible for the secure storage of <COMPANY> or customer data must do so only in conformance to this policy.

Where necessary, data stored must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the <COMPANY> policy on the use of cryptography.

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Disposal

Data disposal describes how data is destroyed. This policy statement is dependent upon the type of media used for data storage.

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process.

The Data Security organization must develop and implement procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques.

Data Security Policy Statement

This section describes the particulars of the data security policy. This section should provide sufficient information to guide the development and implementation of guidelines and specific data security procedures.

Goals

Goals describe the managerial objectives of the policy, and why it is necessary.

This policy has been written with the following goals in mind:

- To educate <COMPANY> users and vendors about their obligation for protection all data assets.
- To ensure the security, integrity, and availability of all <COMPANY> and customer data.
- To establish the <COMPANY> baseline data security stance and classification schema.

Processing Environment

It is often useful to specify the actual environment where the policy applies. This could place limits on the policy as are appropriate to the organization.

The <COMPANY> processing environment that this policy applies to is comprised of:

- *Applications* – Application software is system or network-level routines and programs designed by (and for) system users and customers. It supports specific business-oriented processes, jobs, or functions. It can be general in nature or specifically tailored to a single or limited number of functions.
- *Systems* – A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data, that is used in a production or support environment to sustain specific applications and business organizations in their performance of tasks and business processes.
- *Networks* – A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices) that are used to transport information between systems.

Data Security Responsibilities

It is important that the policy detail the specific responsibilities of each organization and/or identifiable user population. Data security is called out first as it is the primary organization responsible for supporting this policy.

The Data Security organization is responsible for:

- Defining the security requirements, controls and mechanisms applicable to all data assets.
- Defining the methods and guidelines used to identify and classify all data assets.
- Defining the procedures for identifying data owners for all data assets.
- Defining the labeling requirements for all data assets.
- Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- Defining the procedures necessary to ensure compliance to this policy by all <COMPANY> users and vendors.
- Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognized in industry.

The *Data Security, Network Operations* and *Systems Administration* organizations must ensure the activation of all security mechanisms.

Management Responsibilities

It is important that the policy detail the specific responsibilities of each organization and/or identifiable user population. A section particular to management is always a good idea.

Other organizations within <COMPANY> also have various responsibilities for ensuring compliance with this policy, such as:

- All individual organizations must ensure that staff complies with this policy.
- The *Network Operations and Systems Administration* organizations must ensure that adequate logs and audit trails are kept of all data access.
- The Data Security, *Network Operations and Systems Administration* organizations must ensure the activation of all security mechanisms.
- The *Risk Management* organization is responsible for communicating business requirement and issues for business processes and the data those include, to ensure their correct data classification.
- The internal audit organization is responsible for regularly evaluating the data classification schema for consistent application and use.

Other Responsibilities

It is important that the policy detail the specific responsibilities of each organization and/or identifiable user population. Residual responsibilities can be explained last.

Other organizations have responsibilities to comply with this policy, such as:

- All <COMPANY> agents, vendors, content providers, and third party providers that process customer data must have a documented security policy that clearly identifies those data and other resources and the controls that are being imposed upon them.
- All <COMPANY> agents, vendors, content providers, and third party providers that access the <COMPANY> processing environment and its data or provide content to it must have a security policy that complies with and does not contradict the <COMPANY> security policy.
- All agents, vendors, content providers, and third party providers must agree not to bypass any of our security requirements.

Documentation

Documentation is required to enable the day to day efforts necessary to enforce the data security policy. Documentation also ensures that the policy is implemented consistently on all platforms.

This policy requires procedures be developed, managed and performed. As such, written documentation must be developed for all procedures necessary to fulfill this policy including:

- The management of all userids on all platforms.
- The management of all access control lists on all platforms.
- The execution and review of all audit trails.
- All incident response and reporting.
- All other tasks necessary to support this policy.

Policy Review

A policy review should be performed at least on an annual basis to ensure that the policy is current.

It is the responsibility of the Data Security organization to facilitate the review of this policy on a regular basis. Because of the dynamic nature of the Internet, this policy should be reviewed annually. Senior management, Systems administration, and Legal should, at a minimum, be included in the annual review of this policy.

Data Content

Data content is a subject particular to data security. If necessary, limits on the type of data and how they might be used are discussed here.

The nature of specific data content that exists in the processing environment, and the controls that should apply to these, is dependent upon various factors. This policy does not mandate or endorse particular data content. Rather, the business decision process used to evaluate the inclusion or exclusion of particular data content should consider those items listed below. Regardless as to the specific data content that exists in the environment, all aspects of this policy must be enforced. Considerations for evaluating data content include:

- Legal and regulatory obligations in the locales in which we operate.
- Can privacy, confidentiality, security, and integrity of the data be ensured to the satisfaction of customers and legal authorities?
- Is it in line with our business goals and objectives?

- Do customers require or demand access to specific data content.
- What is common local practice? (e.g., pornography is legal in some communities but strongly frowned upon in others.)
- What rules govern the movement across international boundaries of different data content, and do we have in place controls to enforce these rules?

Data Classification

Data classification is a core feature of a data security policy. A well defined data classification schema is essential for a data security policy. This must represent all of the types of data that exist or can exist in your environment. Examples may be a useful component of this section.

Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Customer Data or Proprietary Company Data.

The Data Security organization is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavors, to develop additional data classifications.

All data found in the processing environment must fall into one of the following categories:

- *Public Company Data* – Public company data is defined as data that any entity either internal or external to <*COMPANY*> can access. The disclosure, use or destruction of Public company data will have limited or no adverse affects on <COMPANY> nor carry any significant liability. (Examples of Public company data include readily available news, stock quotes, or sporting information.)
- *Proprietary Company Data* – Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that <COMPANY> is under legal or contractual obligation to protect. The value of proprietary company information to <COMPANY> would be destroyed or diminished if such information were disclosed to others. Most <COMPANY> sensitive information should fall into this category. Proprietary company information may be copied and distributed within <COMPANY> only to authorized users. Proprietary company information disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary company data include company policies, sales plans, and application source code.)

- *Confidential Company Data* – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse affects on <COMPANY> and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Company confidential information must not be copied without authorization from the identified owner. (Examples of Confidential Company Data include company strategic plans or cryptographic keys.)
- *Confidential Customer Data* – Confidential customer data is defined as data that only authorized internal <COMPANY> entities or specific authorized external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse affects on <COMPANY> and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by <COMPANY> (and others) over which they have custodial responsibility but do not have ownership. (Examples of Confidential customer data including customer bank or brokerage account information, cryptographic keys, or other data considered private.)
- *Public Customer Data* – Public customer data is defined as data that any entity either internal or external to <COMPANY> can access. The disclosure, use, or destruction of Public customer data will have limited or no adverse affects on <COMPANY> or the customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by <COMPANY> (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.)

Data Ownership

The concept of data ownership allows for an entity to be declared responsible for the classification of data. This is an essential element of a data classification schema. You should have management direct the determination of data owner, so that the policy reflects data ownership accurately.

In order to classify data it is necessary that an owner be identified for all data assets. The owner of data is responsible for classifying their data according to the classification schema noted in this policy. If an owner cannot be determined for a <COMPANY> data asset, the Data Security organization must act as its custodian. The default classification for all data not classified by its owner must be either confidential customer data or Proprietary company data.

The Data Security organization is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners.

The owner of all customer data is the individual owner who generates or is assigned ownership of that data. (Data such as public key certificates generated by an external Certificate Authority but assigned to a specific customer are considered owned by that customer.

Non-disclosure Agreements

The use of a non-disclosure agreement is a useful tool if data is used outside of the organization. Its use depends upon local custom and legal environment.

On occasion, data assets may need to be released to entities outside of <COMPANY>. When a legitimate business reason exists for releasing sensitive information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

Data Security Principles

The declaration of data security principles allows for a consistent approach to its implementation across various platforms. These are industry standard concepts and lay the foundation for security requirements and detailed procedures. The specific data security principles are dependent upon your organizations business requirements for security services.

<COMPANY>'s business goals, objectives, and needs for security can be derived from three principles: accountability, authorization, and availability. These three principles emphasize the need for security to function properly in <COMPANY>'s processing environment, which is comprised of applications, network, and system resources. Non-compliance with these principles can have serious, adverse, and deleterious affects on <COMPANY>.

In the context of this policy, the following provides the overall concepts or security principles for which all users and vendors are responsible. It is the responsibility of the Data Security organization to define the specific mechanisms necessary to support these principles.

Accountability

Accountability is the concept that every user must be responsible for their actions, so that in the event of any questionable activity or breach of policy, a specific user can be identified. The specific security services that support accountability are identification, authentication, and auditing. For this policy statement, identification refers to a security service that recognizes

a claim of identity by comparing a userid offered with stored security information. Authentication refers to a security service that verifies the claimed identity of the user, for example a password. Auditability refers to a security service that records information of potential security significance.

All network, system, and application events should be attributable to a specific and unique individual. It should be possible to attribute a responsible individual to every event through an identification service and to verify that the individual so assigned has been properly identified through an authentication service. It must also be possible to trace any event so as to reconstruct the time, place, and circumstances surrounding it through an audit service.

In this context identification refers to a security service that recognizes a claim of identity by comparing a userid offered with stored security information. Authentication refers to a security service that verifies the claimed identity of the user, for example a password. Auditability refers to a security service that records information of potential security significance.

Authorization

Authorization is a concept that access to data and system resources should be limited to a need to know basis, and that specific users must be specifically allowed such access. For this policy statement access control refers to a security service that allows or denies a user request based on privilege, group information, or context. The specific security services that support authorization are access control and confidentiality. Confidentiality refers to a security service that prevents disclosure of information to unauthorized parties while the information is in use or in transit, or while the information is being stored or destroyed.

All network, system, and application events must only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity, or from a job classification or administrative privilege based on that individual's identity. The principle of “least privilege” specifies that individuals only be granted permission for actions needed to perform their jobs.

Limiting actions to those properly authorized protects the confidentiality and integrity of data within the <COMPANY> processing environment.

In this context access control refers to a security service that allows or denies a user request based on privilege, group information, or context. Confidentiality refers to a security service that prevents disclosure of information to unauthorized parties while the information is in use or transit, or being storage or destroyed.

Availability

Availability is the concept that system and data resources must be accessible whenever they are needed. The necessity for availability is dependent upon your particular business proposition. The specific security service that supports availability is integrity. For this policy statement, integrity refers to a security service that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery

All permitted activity should operate with reliability. The data necessary to carry out such events must be readily retrieved and correct with high confidence. All results of an event must be completed, unless the event is aborted in its entirety. The results of an event should not depend in unexpected ways on other concurrent events. The security services themselves must be documented and easily administered.

In this context integrity refers to a security service that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery.

Core Security Principles

Your information systems security architecture, policies, procedures, practices, and guidelines should be developed in concert with the principles stated below. The following are the common core security principles recommended by industry best practices.

- *Accountability Principle* – The accountability and responsibility of information systems security should be explicit.
- *Awareness Principle* – Owners, providers, and users of information systems, and other parties should be informed about (or readily able to gain appropriate knowledge of) the existence and general extent of policies, responsibilities, practices, procedures, and organization for security of information systems.
- *Ethics Principle* – Information systems and the security of information systems should be provided and used in accordance with the ethical standards applicable to your operating environment.
- *Multidisciplinary Principle* – Policies, responsibilities, practices, and procedures for the security of information systems should consider all relevant aspects of this effort, including technical (e.g. software and hardware engineering), administrative, organizational, operational, commercial, educational, and legal.
- *Proportionality Principle* – Security levels, costs, practices, and procedures should be appropriate and proportionate to the values of and degree of reliance on the information systems and to the severity, probability, and extent of potential for direct and indirect, tangible and intangible harm.

- *Integration Principle* – Policies, practices, and procedures for the security of information systems should be coordinated and integrated with each other and with other measures, practices, and procedures of the organization to ensure a coherent system of security.
- *Timeliness Principle* – All personnel, assigned agents, and third party providers, should act in a timely, coordinated manner to prevent and to respond to breaches of the security of information systems.
- *Reassessment Principle* – The security of information systems should be reassessed periodically.
- *Democracy Principle* – The security of an information system should be weighted against the rights of customers, users, data owners, data custodians and other individuals affected by the system, and against your rights as the owners and operators of these systems.
- *Certification and Accreditation Principle* – Information systems and information security professionals should be certified to be technically competent and management should approve them for operation.
- *Internal Control Principle* – Information security forms the core of an organization's information internal control system.
- *Adversary Principle* – Controls, security strategies, architectures, policies, standards, procedures, and guidelines should be developed and implemented in anticipation of attack from intelligent, rational, and irrational adversaries with harmful intent or harm from negligent or accidental actions.
- *Least Privilege Principle* – An individual should be granted only enough privilege to accomplish assigned tasks, but no more.
- *Separation of Duty Principle* – Responsibilities and privileges should be allocated in such a way that prevents an individual or a small group of collaborating individuals from inappropriately controlling multiple key aspects of a process and causing unacceptable harm or loss.
- *Continuity Principle* – Information security professionals should identify their organization's needs for disaster recovery and continuity of operations and should prepare the organization and its information systems accordingly.
- *Simplicity Principle* – Information professionals should favor small and simple safeguards over large and complex safeguards.
- *Policy-Centered Security Principle* – Policies, standards, and procedures should be established as a basis for managing the planning, control, and evaluation of information security activities.

Summary

This template provided a brief description of recommended security policy topics and an overview of core security policies. In addition, this template outlined a sample Data Security Policy and Statement and provided commentary explaining the details of each security topic and why it was chosen for the particular policy. Finally, a detailed list of security policy principles was described.

This template was built from the Sun BluePrints article, *Developing a Security Policy* (12/01), by Joel Weise and Charles R. Martin. The article is available from:

```
http://sun.com/blueprints/1201/secpolicy.pdf
```

Author's Bio: Joel Weise

Joel Weise has worked in the field of data security for over 20 years. As a Senior Security Architect for Sun Professional Services, he designs system and application security solutions for a range of different enterprises from financial institutions to government agencies. He specializes in cryptography and public key infrastructures. Prior to joining Sun, Joel was a Senior Project Manager for Visa International. There he was responsible for developing cryptographic standards, designing key management and cryptographic systems and architecting security solutions for chipcard, Internet, and other new products.

Author's Bio: Charles R. Martin

Charles R. Martin has been in the computer business for more than 30 years, and involved with computer security since 1983. He was the original architect for a DARPA B3/A1 X server, developed methods for covert channel analysis in full-scale UNIX kernels, and has co-authored several chapters in the NRL handbook on trusted system evaluation. He is currently a Senior Java Architect with Sun Microsystems in the Sun Java Center developing methods for quantitative analysis of distributed system architectures, and a member of the graduate faculty at the University of Colorado in Boulder.