Security Policies

University at Albany, SUNY
Spring 2004
Policies
Definitions

• A *policy* is a plan or course of action of an organization intended to influence and determine decisions, actions, and other matters.
  – Policies are organizational laws - they dictate acceptable and unacceptable behavior within the context of the organization’s culture
  – *Practices, procedures and guidelines* explain how to comply with policies

• *Standards* are detailed statements of what must be done to comply with the policy.
Policies
Definitions

• A *Security policy* is a set of rules that protect an organization’s assets

• An organization’s security policies should reflect
  – The organization’s goals in creating the policies, and
  – The context in which the organization operates.
    • The computer and network environment, and
    • The organizational environment.
      – Private or Public
      – Applicable laws, rules and regulations
      – Organizational culture.

• Unless these things are taken into account, the policies may be inappropriate.
Information Security Policies

Definitions

• An information security policy provides rules for protection of the information assets of an organization.

• Four types of security policies are required.
  – Security Program (General) security policies
  – Issue-Specific security policies
  – Systems-Specific security policies
  – An Acceptable Usage Policy, which summarizes parts of the first three.
Information Security Policies

Security Program Policy

• The Security Program Policy is an executive level document.
  – Drafted by the Information Security Officer.
  – Generally 2 to 10 pages in length.

• It shapes the philosophy of security in the IT environment.

• It defines the
  – Purpose,
  – Scope.
  – Constraints, and
  – Applicability

of the security program in the organization.
Information Security Policies

Security Program Policy

• The Security Program Policy assigns responsibilities for the various areas of security, including
  – System administration,
  – Maintenance of security policies, and
  – Practices and responsibilities of users.

• Addresses compliance with the security policy
  – General compliance to ensure meeting security requirements,
  – Use of specific penalties and disciplinary actions.
Information Security Policies

Issue-Specific Security Policy

• Issue Specific Security Policies are guidelines to instruct employees how to use technologies and processes.

• As the name implies, they are very specific policies. They
  – Address specific areas of technology,
  – Require frequent updates,
  – Contain statements of the organization’s position on specific issues
Information Security Policies

Issue-Specific Security Policy

• Issue-Specific Policies may cover:
  – Electronic Mail,
  – Use of Internet,
  – C of computers to defend against worms and viruses,
  – Prohibitions against hacking or testing organization security controls,
  – Home use of company-owned computer equipment,
  – Use of personal equipment on company networks,
  – Use of telecommunications technologies, and
  – Use of photocopy equipment.
Information Security Policies

System-Specific Policy

• System-Specific Policies are usually coded standards and procedures used while configuring or maintaining systems:
  – For example, an access control list that defines which users may access a particular system or data.
Information Security Policies

System-Specific Policy

• System-Specific Policies can be organized into two general groups:
  – *Access Control Lists*: Lists, matrices and capability tables governing the rights and privileges of a particular user to a particular system. They
    • Regulate access, *e.g.*, who, what, when, where, and how.
    • Regulate privileges, *e.g.*, read, write, create, modify, delete, compare, copy.
  – *Configuration Rules*: The specific configuration information entered into security systems to guide their behavior.
    • They govern the configuration of systems such as
      – Firewalls,
      – Intrusion detection systems (IDSs), and
      – Proxy servers.
Information Security Policies

Defining Policies

• When creating Information Security Policies, it is important to identify the relevant areas, operations and issues of the organization.
• This is unfortunately time consuming.
• A starting point for identifying important areas can be the results of a Risk Analysis.
Physical Security
Facility Construction

Examples

• Issue-Specific policies can be created to cover standards for new and existing computing facilities.

• For example,
  – Computing facilities shall be of sufficient size such that [...] and be located on any floor other than the ground floor, with multiple entry doors and more than one fire exit.
  – Computing facilities shall be located on a floor capable of solid construction with multiple entry doors, fire exits, and that allows for access to redundant power supplies.
Locks and Barriers
Support

- **Environmental Support**
  - The areas used for the servers shall have sufficient environment controls that include temperature and humidity controls to protect against static electricity.

- **Inventory Maintenance**
  - Equipment should be tracked and identified with the help of metallic equipment tags or some other tamper-proof material.
Facilities
Access Controls

• Building Access Controls
  – Facilities Access controls shall be maintained through an automated identification process that includes procedures to add and remove people from databases or lists that control access to the organization’s facilities.
  – These procedures must be auditable.
  – Further, records shall be kept as to who is allowed to access each area of the facility and logs maintained that can identify everyone who has entered and exited each secured area.
Facilities

Access Controls

• Restricting Access to Computer Facilities
  – Access to storage areas, where magnetic tapes, extra disks, and sensitive documentation is stored, should be restricted.

• Visitors
  – Visitors shall be required to provide positive identification before entering any company facility.
  – Once allowed inside, an employee shall escort the visitor during their time on premises.
Contingency Planning

Mitigation Measures

• Emergency Response Plans
  – The System Manager shall maintain an emergency and disaster response plan that will discuss what will happen in the event of a disaster to organizational facilities.
  – This plan shall ensure the integrity of data and the ability to recover quickly when the disaster has passed.
  – Any plan created from this policy shall include provisions to preserve life and prevent bodily injury by anticipating multiple scenarios and allowing employees to choose not to participate when they are in immediate danger.
Contingency Planning (Contd..)

Mitigation Measures

• Disaster Recovery
  – This disaster recovery plan shall undergo a periodic review in a reasonable time frame with a maximum duration between reviews of one year.
  – The review and audit procedure shall include a plan to test the procedure.

• Security Alerts and Alarms
  – An alert system needs to be in place that will notify the appropriate people of disruptions to monitored systems.
General Computer Systems Security
Measures to be adopted

• Preventative Maintenance
  – A preventative maintenance plan needs to be in place to avoid the risk of significant portions of the business process being disrupted.
General Computer Systems Security

Measures to be adopted

• System Availability
  – Procedures shall be established to allow a limited use of controlled overrides of system resources.
  – These procedures shall establish a path of authority of the decisions for the controlled overrides that can be logged and reviewed.
System & Network Configuration Audits

Auditing Guidelines

• The Operations Manager shall conduct a system and network configuration audit at least once every calendar year.

• The Operations Manager may conduct audits at other times as deemed necessary.
System & Network Configuration Audits

Auditing Guidelines

• The Systems Manager shall author a plan to audit the system and network configuration.
• This plan shall include procedures for auditing the hardware configuration, connectivity of the network, and installed systems components.
• The plan shall be approved by a committee consisting of the Systems Manager (and other department heads).
• This committee shall review these procedures annually or more often as needed.
• The audits shall be conducted at least once every calendar year.
• The Systems Manager may conduct audits at other times as deemed necessary.
Staffing Considerations
Points to be noted for hiring

• Mandating the maintenance of an inventory of key technical jobs and cross-training of personnel.
• Other policies about hiring and security clearances are usually left to the Human Resources Department.
Network Security
Network Addressing and Architecture

Setting up a secure network

• Network survivability ensures that the network operates and transmits information during failures, attacks, or other mishaps.
• Policies that support diligent planning, attention to network addressing issues, and network expansion can assist in improving survivability.
• Dictate that as systems fail, that they fail in as secure a way as possible.
  – E.g. that a firewall, when it fails, denies all access, rather than allowing all access.
Network Addressing and Architecture

Setting up a secure network

• Network Planning

• Access to confidential or critical data can be limited by isolating the support systems and networks from general network traffic using technologies like restricted gateways, firewalls and air gaps.
Network Addressing and Architecture

Setting up a secure network

• For example, in some situations sensitive information about human resource data must be protected by law.

• To ensure this, we can have a policy like the following:
  – Human resources, accounting, and other administrative support systems shall be physically partitioned from the general network in such a manner to control the flow of information to and from those systems.
Network Addressing and Architecture Cont’d.

Setting up a secure network

• Network Addressing
  – There are two common ways to mitigate the problem of someone pinpointing which systems might be active and focusing the attack.
    1. Through Domain Name Service configuration (DNS).
    2. Network Address Translation (NAT).

• The general idea is to configure the network so as to reveal a minimum of information to the outside world.
Additional Addressing Concerns

System protection

• It is common to use static or pre-defined addresses even if they are resolved using DHCP.
  – This allows mapping of actions to a specific machine.
• Sample policies could read:

  Network addresses shall be predefined for every system and network device and may be preloaded or resolved when logged in to the network. Network address servers and those used to resolve addresses shall be protected in accordance with best practices appropriate for that device.
Policies for expanding the network
Planning for growth

• As technology becomes more flexible and pervasive, it is inevitable that the network will need to be expanded.
  – A few sample policies to govern this can be:
    • Procedures shall be created describing any reconfiguration of the organization’s network.
    • These procedures shall include changes directly to all internal and external access points.
Network Access Control

Gateway Installation

- *Gateways* are the points where network traffic is transferred from the organization’s network to another network.
  - Any gateway proposed to be installed on the company’s network that would violate policies or procedures established from these policies shall not be installed without prior approval of the Information Security Management Committee.
  - Applications that require gateway services shall be authenticated to the network.
  - If the service itself cannot be authenticated, services carried through the gateway shall be subject to authentication policies.
Network Access Control

Gateway Installation

• Modems may need to be in the policy.
  – All telephone access to the network needs to be centrally protected by strong authentication controls.
  – Modems shall be configured for dial-in or dial-out access but not both.
  – The Network Administrator shall provide procedures to grant access to modem services.
  – Users shall not install modems at any location on the network without appropriate review and authorization by the Network Administrator.
Authentication
Login Security
Policies for authentication

• Login Requirements and Procedures
• A policy to create usernames could be:
  – User identification names shall consist of the 5-digit employee identification number assigned by the Human Resources Department and will be prefixed by a single letter.
    • Hmm, why might this be a bad example?
Login Security
Policies for authentication

• Another example of restrictions on system usernames could be:
  – System and default usernames loaded and required by the operating system shall be assigned a password different than what was loaded.
  – Usernames required for services without login requirements shall be configured to not allow logins.
  – Usernames for services not in use shall be deleted from the system.
Login Security Contd.
Policies for authentication

• Guests and Other Users
• An organization should have a policy on Guest users:
  – The administrator shall provide procedures for granting, revoking, and reviewing access to guests and other non-organizational users.
Login Security Contd.

Policies for authentication

• Guests and Other Users

A series of policy statements that might be used are:

– Guests and other non-organizational users shall be recommended for access to the network and its resources by an organizational sponsor, and that access granted by a designated Systems or Network Administrator.

– The sponsor shall familiarize the user with the organization’s security policies and procedures, with the understanding that they are responsible for monitoring the guest user.

– Guest usernames shall be assigned only for the duration that access is required.

– Usernames shall be revoked following the end of the access requirement.
Login Security Contd.

Policies for authentication

• *Login Banners* are the information that are displayed on the screen when the login prompt is presented.
  – All login screens, displays, and other banners appearing during the login or authentication process shall not contain information identifying anything about the operating environment.

• For legal reasons, it may be necessary to have specific warnings and prohibitions in the login banners.
Login Security Contd.

Policies for authentication

• *Login controls* are those that assist the authentication process.
  – Login services shall provide for positive authentication that will ensure that a legitimate user is allowed access to the system or network environment.
Setting Session Restrictions

User session security

• Once a user is logged in, we may want to require a number of restrictions on the user’s management of his or her session.
  – This would depend on the systems and what various users are required to do.
Setting Session Restrictions

User session security

• A solid policy statement, for a combination of session restrictions, could be:
  – Users shall log off and secure workstations when not in use.
  – Administrators shall create procedures to ensure that unused workstations are secured by logoff or other means when they remain idle for a period of time determined reasonable by a review of the procedures.
Setting Session Restrictions Contd.

User session security

• Special Privileges
  – Procedures for special privileges shall be written to ensure that they can be administered properly within the organization’s technical environment.
  – These procedures shall define how access requirements will be administered, managed, or reviewed.

• Ensure that the policy addresses review and removal of privileges.
  – This to keep people from retaining privileges they no longer need.
Passwords
Rules for password handling

• Valid Passwords
  A sample statement for defining valid passwords can be as follows:
  – Each user account shall have its own password.
  – A valid password shall consist of a combination of letters, numbers, or special characters; be comprised of at least 8 characters; and remain valid for 90 days from when it was last changed.
  – A password may not be reused for at least 24 months from its last use.
User Interface

Rules for password handling

• Several concepts can be put together in a policy statement like:
  – Password interfaces shall allow users to enter their passwords without demonstrating any of the characteristics of their entry.
  – Those passwords shall not be transmitted over the network in a readable form.
Access Controls
System Access

• We first need to find out where to use computer systems access controls and which systems require username/password-based access control.

• We can then frame a policy like this to govern new systems:
  – Information owners wishing to install new systems or software in support of new or existing business requirements that require access control shall author a policy for that access control prior to installation.
  – New policies shall be subject to the same review processes as existing policies.
Telecommuting and Remote Access

Outside Access

• A policy ensuring that a employee who is working off-site maintains the company’s policies and procedures can be something like this:
  – The employee accessing the organization’s network remotely shall abide by security policies and procedures to protect the organization’s equipment, data, and network access as if they were working on premises.

To further strengthen the policy, we could add:
  When working off-site, users shall use only properly licensed software, submit to prescribed backup procedures, and comply with all operating procedures.
Telecommuting and Remote Access Facilities

Outside Access

• Dial-up Security
  – The telephone numbers used on incoming modem lines shall not be published in any directory that may be accessed by anyone other than those authorized for access.
  – Those accessing the network through dial-up modems shall be required to undergo an additional authentication step in order to be granted access.
Network Security Highlights

Summary

• Security Policies for network planning will guide network architects to isolate systems with secret or critical data so that access can be better controlled.

• Network addressing policies cover how much information on the configuration of the network is available outside of the organization.
  – Configure DNS to hide machine names, and Network Address Translation (NAT) to hide addresses.

• Policies should mandate procedures for expanding or changing the network.

• Issues such as static and dynamic addresses etc., also should be included in network addressing policies.
Internet Security Policies
Policies for Internet Security

• The aim of writing architectural policies for securing Internet access is to ensure that security is a consideration while allowing the doorway to service Internet traffic without hindering access.

• There are many issues having to do with access and protection:
  – A firewall is a device that helps manage the traffic by enforcing policy rules regarding what is allowed in and out of the network.
  – A DMZ is an area where machines providing external services reside on your network.
Architectural Options
Viable Policies

- The DMZ assumes that an organization supports its own internet service using some type of persistent connection. In reality, there might be different types of services that require different policy options. For example, if your organization uses a hosting service, then architectural policies might not be necessary. When you write policy statements for your organization’s environment, make sure that they can be enforced – especially given that you might not be able to enforce the architecture provided by your Internet Service Provider (ISP).
Allowable Services

Committee Approval

• Services supported by the Internet gateway shall be defined by a committee responsible for verifying the necessity of allowing the service through the gateway and appropriate business requirements.

• Can involves some very technical questions like policies for admitting/denying UDP and ICMP packets.
Administrative Responsibilities

Policy Enforcement

• Administrators shall enforce these policies in accordance with established procedures. Administration procedures shall include monitoring and preserving of information in a manner that will allow appropriate action to be taken. These procedures shall include, but not be limited to, preserving evidence for disciplinary actions for employees and legal action to be used for external violators.

• Users who access the Internet shall undergo a training program that will explain company policies and their responsibilities while representing the organization online. Users shall not use Internet resources unless they have completed the required training program.
Transmission of Sensitive Information

User Control

• Users shall not transmit any information that discloses the intellectual property or business intelligence of the organization. Users shall not purposely transmit documents or other data to customers or others outside of the organization without taking appropriate precautions.
World Wide Web Policies

Securing Web Servers

- All systems hosting proprietary and customer data that support the web server shall not be installed on the same network segment as the web servers. These support servers shall be installed in such a way where only the web servers can gain access.

- Web servers shall only run verified and maintained programs and scripts that execute as part of the common gateway interface (CGI) with the web service. All other program execution shall be performed on other systems not associated with the web services where these scripts act as a proxy for that execution.
World Wide Web Policies

Securing Web Servers

• Support programs for web servers shall undergo a thorough review of all components.
• Web servers shall be installed with and configured to only provide the services necessary to support the operating environment.
World Wide Web Policies Cont’d.

Securing Web Access

Filtering Applets

• Both technologies, Java and ActiveX, have created applets which have serious security concerns, but applets have also been used for customer support, creating chat rooms, and enhancing e-commerce initiatives.

Privacy Policy

• Web Servers, shall include a Privacy Policy that explains what information is being collected and what the organization will do with that data.
World Wide Web Policies Cont’d.

Securing Web Access

• Users accessing the Internet shall not visit sites that violate the law or could be offensive to fellow users.

• Employees of the organization shall not be allowed to create unofficial web sites on the organization’s network. These web sites shall be accessible only from within the organization.
Data and File Transfers

Security Measures

• Data and process owners shall evaluate all applications to ensure that file and data transfer security is maintained as appropriate for their business process.

• Data and process owners shall ensure that the identities of all users of proprietary data are verified to be valid users.
VPNs, Extranets, Intranets, and Other Tunnels

Security Measures

• Data and process managers who employ tunneling shall ensure the transmission cannot be read anywhere but the remote system by employing encryption.
Electronic Commerce
Considerations

• The following principles need to be considered when we need to write policies for e-commerce.
  – Storage of Data
  – Identification and Authentication
  – Secure Data Transmission
  – Processing of Orders
Email Security Policies
Administration of Email
Handling and Management of Electronic Mail

• As with many things, an e-mail policy is necessary.
• The next couple of slides give an example policy.
• Different organizations may take radically different tacks on e-mail policies.
  – Organizational goals
  – Management styles
  – Constraints on what is legally or contractually possible.
Administration of Email

Handling and Management of Electronic Mail

• Network and Security Administrators shall architect the email system in a way that will allow the proper delivery of messages both within the organization and to the Internet.

• The organization shall retain and archive all email messages that pass through its servers.

• The organization shall retain that offline storage medium for at least two years but may regain it for longer periods at the discretion of management.

• The organization shall alter its policy to comply with contractual obligations on an as-needed basis and without policy review.
Scanning Email
Handling and Management of Electronic Mail

• Scanning Email
  – The organization shall scan every email message that passes through its server to check for computer viruses, worms, or other executable items that could pose a threat to the security of the network.
    • Servers do spam filtering as well?
  – Email messages sent to and from users shall not exceed a defined size (e.g. 40 kilobytes).
Use of Email for Confidential Communication
Handling and Management of Electronic Mail

• Encrypting Email for Confidentiality
  – Proprietary information sent to users outside of the organization shall be encrypted prior to its transmission.
    • An interesting point - is this a practical policy, or is it wishful thinking?

• Digitally Signing Email
  – Any request for proprietary information shall be digitally signed and that signature verifiable.
Viruses, Worms and Trojan Horses
Viruses, Worms, and Trojan Horses

Virus Protection

• All users shall have anti-virus protection software installed before connecting the systems to the network.
• Users shall participate in keeping this software updated and shall not disable its facilities. If the anti-virus software is disabled for any reason, such as the installation of new software, the user shall perform a full-system scan before using the system again.
Establishing the Type of Virus Protection

Virus Protection

• Testing for Viruses
  • Anti-virus software shall be installed and configured on each of the organization’s networked systems in such a way to provide constant scanning for viruses and periodic updates as defined by administrators.
Establishing the Type of Virus Protection

Virus Protection

• System Integrity Checking
  – All systems connected to the organization’s network shall undergo periodic integrity checking for virus infection of its operating systems and support software.

• Distributed and Removable Media
  – Users loading any data or programs from an external media source shall scan that media for viruses before loading.
Rules for Handling Third-Party Software

Virus Protection

• All third-party data and programs must be tested for malicious code, etc. before being allowed in the organization’s systems.

• The third-party data and programs shall be loaded on a special purpose, isolated system that scans the data/programs for viruses, bugs, or other malicious problems.

• Only after passing the scan can the third-party material be used on the organization’s systems.
User Involvement with Viruses

Virus Protection

• Users shall not knowingly create, execute, forward, or introduce any computer code designed to self-replicate, damage, or otherwise impede the performance of any computers memory, storage, operating system, or software. Users violating this policy may be disciplined or dismissed and will be reported to proper legal authorities.

• Not too likely, but this is one you are going to want in your back pocket in case something comes up.

• Also other, related policies on other anti-social behavior.  
  – Or maybe a general blanket policy.
Encryption
Encryption
Securing Data through Encryption

• Managing Encryption
  – Management shall approve all use of encryption within the organization. Prior to approval, management shall verify that its use complies with all applicable laws and regulations.
Encryption

Securing Data through Encryption

• Handling Encryption and Encrypted Data
  – All data shall be classified based on usage. The criteria shall include considerations for the sensitivity of the data, where it is stored, and how the data is transmitted.
  – Archive and backup data shall not be encrypted. Sensitive data shall be stored in a manner consistent with policy.
    • Does this make the backups a vulnerability since they’re unencrypted?
  – All original data shall be deleted or its media destroyed after it is encrypted. Memory and storage used by encryption processes shall be thoroughly erased before being released.
Key Generation Consideration

Securing Data through encryption

• All materials used in generating encryption keys shall be destroyed following their use. All memory and storage devices shall be thoroughly erased or destroyed as appropriate.
Key Management
Securing Data through encryption

- Encryption keys shall be disclosed only when required for exchange or by law.
  - Key Storage
    - Keys shall not be stored on the same media as the protected data.
    - All management of public key/asymmetric encryption keys shall not be transmitted using the same network that will carry encrypted data. All symmetric encryption keys shall be physically exchanged and not transmitted across any network.
Software Development Policies
Software Development Processes
Policies for governing Software Development

• If your organization develops its own software, then that introduces the need for a whole new set of policies.
• These policies govern the software development process.
• Many organizations have general policies, standards, *etc.* for software development.
  – Here we’re interesting in ones that focus on ensuring security in software developed in-house.
Software Development Processes
Policies for governing Software Development

• Identifying Software Development Responsibilities
  – All software development and acquisition requirements shall include security requirements consistent with these policies. The author of the overall requirements shall be responsible for ensuring that security requirements are specified.
  – All programmers involved in development and maintenance shall subscribe to all policies, procedures, and other development conventions.
Software Development Policies

Rules for governing Software Development

– No software development shall occur without formal specifications. These specifications shall include requirements for security and privacy of the data being collected and processed.

– All software shall verify and acknowledge user input, regardless of outcome.

– All software shall check and verify boundaries of data transferred to and from blocks of memory to prevent overwriting of critical data and programs.
Access Controls in Software
Policies for governing Software Development

• No software shall be installed or considered for installation that includes shortcuts, trap doors, or any path that may circumvent security.
• No software shall be installed or considered for installation that includes special access privileges for developers.
• All access privileges and controls built into custom software shall conform to the standard administrative controls as outlined by these policies and associated guidelines.
Other Policy Considerations
Policies for governing Software Development

• All software development shall use one programming language consistent across projects. Software development shall consider reusability a secondary goal of the project.
• All software development shall use a single naming convention for all production files.
Authentication Design Rules

Password Protection

• Identification and Authorization of custom developed software shall use and integrate the mechanisms of the operating system, database, or supporting software system in its design and deployment.

• Passwords shall not be transmitted in clear text across the network without having being encrypted.

• Passwords shall not be stored in clear text on accessible storage devices.

• Passwords shall never be a static value stored within the program (hard-coded).

• Memory used for deciphering and checking passwords shall be cleared once processing is completed.
Testing and Documentation

Acceptance methodologies

• All custom development shall be tested and documented before being installed into the production environment.
• Generating Test Data
  – Data used to test software shall be generated from production data to properly simulate real situations. This data shall be sanitized to remove sensitive or proprietary information prior to its use.
• Testing and Acceptance
  – Software accepted from testing shall include a plan to install it into the production environment. This plan shall include procedures for uninstalling the software should it become necessary.
  – Installation shall not occur without notifying users to the procedures and error-reporting requirements.
  – Software accepted for installation shall not be installed without appropriate operating documentation.
Testing and Documentation
Acceptance methodologies

• Documentation Requirements
  – Software development procedures shall include user and technical documentation that describes how the software works; how it is operated; its inputs and outputs; interfaces with the system and other components; and the security controls it uses.
Revision Control and Configuration Management

Steps for Configuration Management

• A configuration management program shall be established to maintain the configuration of all production systems, including operating systems, off-the-shelf software, and security controls.

• Revision Control Request Procedures
  – Revision control and configuration management shall establish a formal change control procedure for all production systems. These procedures shall include mechanisms for written change requests, maintaining the sources of development software installed on production systems, and a review of security controls.

• Configuration Management and Security Fixes.
  – Configuration management shall have procedures in place to test and install security fixes from developers and vendors.

• Configuration Management and Maintenance.
  – All maintenance on custom developed software shall be performed on the programs source and not its associated binary.

• Testing Before Installation
  – All software shall undergo testing and acceptance prior to using in a production environment. This policy shall include vendor-supplied software and patches as well as those developed in-house.

• Installation Procedures
  – Configuration management procedures shall include procedures to install and roll-back to a previous version should problems occur.
Revision Control and Configuration Management

Steps for Configuration Management

• A configuration management program shall be established to maintain the configuration of all production systems, including operating systems, off-the-shelf software, and security controls.
  – Revision Control Request Procedures
  – Configuration Management and Security Fixes.
  – Configuration Management and Maintenance.
  – Testing Before Installation
  – Installation Procedures
Revision Control and Configuration Management

Steps for Configuration Management

• Revision Control Request Procedures
  – Revision control and configuration management shall establish a formal change control procedure for all production systems. These procedures shall include mechanisms for written change requests, maintaining the sources of development software installed on production systems, and a review of security controls.
Revision Control and Configuration Management

Steps for Configuration Management

• Configuration Management and Security Fixes.
  – Configuration management shall have procedures in place to test and install security fixes from developers and vendors.
Revision Control and Configuration Management

Steps for Configuration Management

• Configuration Management and Maintenance.
  – All maintenance on custom developed software shall be performed on the programs source and not its associated binary.
Revision Control and Configuration Management

Steps for Configuration Management

• Testing Before Installation
  – All software shall undergo testing and acceptance prior to using in a production environment. This policy shall include vendor-supplied software and patches as well as those developed in-house.
Revision Control and Configuration Management

Steps for Configuration Management

• Installation Procedures
  – Configuration management procedures shall include procedures to install and roll-back to a previous version should problems occur.
Third-Party Development

Interaction with Outside Parties

• Policy to Guarantee Integrity
  – All agreements with third-party software developers shall include a statement of integrity. This statement shall include assurances of no undocumented features and that the software developed shall not include backdoors, trapdoors, or other mechanisms to circumvent security.
  – Restriction Commercial Distribution
    • Where possible, third parties developing software for the organization shall not sell or redistribute this software. Documentation associated with this software shall not be distributed.
  • Escrow for Third-Party Software
    – All third-party development agreements shall include a provision to place a copy of the source and executable programs into escrow. These provisions shall allow the organization to access that escrow should the third party fail to maintain the software.
Intellectual Property Issues
Creating Policies for Intellectual Property

• For those organizations without an intellectual property policy, it might be worth the resources to ensure your organization creates one. Because these policies must comply with the appropriate laws, which can be complex, your organization should employ an attorney whose specialty is intellectual property to help with this endeavor.
  – Or, you may already have one.
Acceptable Use Policies
Acceptable Use Policies

What is a AUP?

• An Acceptable Use Policy (AUP) is a document that summarizes an organization’s overall policy for its users.

• It is a summarized version that contains parts of the organization’s policies outlining the user’s security responsibilities.
  – Ideally, the AUP should only be a few pages.

• The ‘AUP’ can be seen as a “quick start” document to allow users to read the full policy later.
The structure of the ‘AUP’

Sections of the AUP

• Introduction and Purpose.
• Recognize a “Higher Authority.”
• User Responsibilities.
• User login responsibilities.
• Use of systems and network.
• Internet user responsibilities.
• Organization’s responsibilities and disclosures.
• Common-sense guidelines about speech.
Compliance and Enforcement
Laying down the rules

• Testing and Effectiveness of the Policies
  – All users of the organization’s network and systems shall undergo security-awareness training to explain these security policies prior to being allowed access.

• Security, Systems and Network
  – Administrators shall maintain records of all security violations.
  – Security Administrators shall maintain Risk Acceptance Memos for each waiver granted to these policies.
Publishing and Notification

Requirements of the Policies

• The Human Resources Department shall be responsible for publishing these Information Security Policies and all updates on the organization’s intranet to make it easily accessible by everyone.

• When these policies or updates are published, the Human Resources Department shall notify every user that the policies have been published and how they may be accessed.

• The Human Resources Department shall be responsible for providing each department and others without access to the intranet a printed copy of these policies at the same time as the publishing of the electronic version.
Monitoring, Controls, and Remedies

Policy Requirement

• Monitoring
  – Management shall be allowed to monitor all systems activities and network traffic to enforce the provisions of these policies. Management shall be allowed to assign monitoring and other duties to appropriate administrators.
Monitoring, Controls, and Remedies

Policy Requirement

• Controlling
  – Management shall install controls consistent with the requirements of these policies.
  – Management and assigned administrators shall have the responsibility of testing access controls and the network of vulnerabilities.
  – Management and assigned administrators shall have access to the tools that can help manage and test information security.
  – Users shall not have access to these tools on the organization’s network.
Monitoring, Controls, and Remedies
Cont’d.

Policy Requirement
• Remedies
  – Any conduct which adversely affects the ability of others to use the company’s systems and networks or which can harm or offend others shall not be permitted.
  – Management shall have the right to revoke any user’s access privileges and terminate their association with the organization at any time for violations of this policy or conduct that disrupts the normal operation of the organization’s network and computing systems.
  – Management shall have the right to exercise their options under the appropriate criminal and civil laws to seek legal remedies from anyone who uses, abuses, or attacks the organization’s network and information systems in a manner that would be in violation of the law and these policies.
Administrators Responsibility

Follow Up

• Users whose association with the organization has been terminated shall have their access privileges to the organization’s resources immediately revoked. Administrators shall arrange for the programs and other data used by these users archived.
Logging Considerations
Administrators Responsibilities

• A generic set of policy statements to support this can say
  – Administrators shall review the system and other logs on a regular basis.
  – Only authorized users shall review log files.
  – Administrators shall take appropriate precautions to prevent logs from being deactivated, modified, or deleted.
  – Administrators shall follow appropriate procedures when they discover violations of these policies or network security.
Reporting of Security Problems
Keeping track of Security issues

• Handling of Information Security Incident Reporting
  – Administrators and users shall report all violations to these policies and associated procedures using the designated reporting procedures.
  – Administrators shall take reports from all outside sources seriously and investigate their validity.
  – Administrators shall monitor public disclosure organizations that report incidents, bugs, and other problems that could affect the security of the organization’s network and systems.

• Auditing and Data Capturing
  – Data regarding information security violations and incident handling shall be retained so that it may be used during the analysis of the information security policies.
After Computer Crimes Are Committed

Law Enforcement

- To write policies in this area, all aspects of dealing with the law enforcement community should be reviewed to determine policy requirements.
The Policy Review Process
The Policy Review Process

Periodical Updates

• Periodic Reviews of Policy Documents.
  – Information Security Policies shall undergo a review every six months.
    • Or annually, *etc.* depending on what is both desirable and realistic.
  – Management shall form an *ad hoc* review committee to create, update, or review policies when significant changes are necessary prior to the regular review.
The Policy Review Process

Contents of the Policies

• What the Policy Reviews should include:
  – The information collected during the authoring process will continue to be valuable.
  – Data collected while enforcing the policies and procedures that were created as a result of these policies.
  – The information collected from a risk assessment or audit.
  – Management can bring the business process and business intelligence as input.
The Review Committee
Composition of the review Committee

• Ideally, the review committee will consist of representatives from all stakeholders affected by the policies.

• Smaller organizations may not be able to commit the resources necessary to do a review. These organizations can try creative methods rather than organizing meetings.
Acceptable Usage Policy

Sample

• **Case:** A sample of an Acceptable Use Policy for an organization with more than 250 users. The organization uses mainframes, UNIX servers, and PCs on the desktop. All the offices are tied together using private lines.

• This document sets forth the policy of ______ (the Company) with regard to the use of, access to, review, and disclosure of various electronic communications, including those sent or received by Company employees.

• This information systems policy applies to all individuals using the Company's computer and network systems, including employees, subcontractors, and consultants. For the purposes of this document, "electronic communications" includes, but is not limited to, the sending, receipt, and use of information through the corporate electronic information network, the Internet, voice mail, facsimiles, teleconferencing, and all other online information services.
Acceptable Usage Policy Cont’d.

Sample

• **Information Systems are for Business Purposes**
  Information systems offered by the Company are provided to its users for the primary purpose of Company-related use.

• **Monitoring and Privacy**
  Electronic communications through the Company's information systems are the property of the Company to assist it in carrying out business. The Company treats all electronic communications sent, receive, or stored as business messages, including those for personal use.
Acceptable Usage Policy Cont’d.

Sample

• **Data Retention Policy**
  The Company will retain email messages and any backup of such email for six months. Other computer system backups will be stored for only one year, or longer if required by contract.

• **Prohibited Activity and Use of Good Judgment**
  Use of electronic communications to engage in any communication or action that is threatening, discriminatory (based on language that can be viewed as harassing others based on race, creed, color, age, sex, physical, handicap, sexual orientation, or otherwise), defamatory slanderous, obscene, or harassing is prohibited. Electronic communications shall not disclose personnel information without authorization. The destruction or alteration of electronic communications with the intent to cause harm or injury to the Company or an employee of the Company is strictly prohibited.
Acceptable Usage Policy Cont’d.

Outline

• Intellectual Property and Licensing
  The ease of copying through various electronic communications systems poses a serious risk of intellectual property infringement. Each user must be aware and respect the rights of others.

• Virus Protection
  Users may not knowingly create, execute, forward, or introduce any computer code designed to self-replicate, damage, or otherwise impede the performance of any computer's memory, storage, operating system, or software.
Acceptable Usage Policy Cont’d.

Outline

• **Disciplinary Action**
  Management reserves the right to revoke any user's access privileges at any time for violations of this policy and conduct that disrupts the normal operation of the company's information systems.

• **Acknowledgment**
  I acknowledge that I have read and will abide by the Company's Information Security Policy.
E-mail Policy

Sample

• **Administering Email**
  The Company is responsible for creating and managing an infrastructure that can support the safe and successful delivery of email within the Company and to customers, partners, and others via the Internet.

• **Email Virus Protection**
  Email that has been found to be infected with a virus, worm, Trojan Horse, or contains another executable item could pose a threat to security will not be delivered to the user.

• **Archiving Email**
  All email is retained and archived. The archive will reside on a server controlled and managed by network and security administrators with access limited to security management, human resource management, and the Company's executive management.

• **User Responsibilities**
  Email is the electronic equivalent of a postcard. Anyone can read its contents along the deliver path.
E-mail Policy Cont’d.

Sample

All users of the Company's email service will follow and respect the *Ten Commandments of Email*:

• Thou shalt demonstrate the same respect thy gives to verbal communications.
• Thou shalt check thy spelling, thy grammar, and read thine own message thrice before thou send it.
• Thou shalt not forward any chain letter.
• Thou shalt not transmit unsolicited mass email (spam) unto anyone.
• Thou shalt not send messages that are hateful, harassing, or threatening unto fellow users.
• Thou shalt not send any message that supports illegal or unethical activities.
• Thou shalt remember thine email is the electronic equivalent of a post card and shalt not be used to transmit sensitive information.
• Thou shalt not use thine email broadcasting facilities except for making appropriate announcements.
• Thou shalt keep thy personal email use to a minimum.
• Thou shalt keep thy policies and procedures sacred and help administrators protect them from abusers.
Administrative Policy

Sample

User Training
- All users of the Company's networks and systems shall undergo security awareness training to explain these security policies prior to being allowed access.

Publishing and Notification
- The Human Resources Department shall be responsible for publishing the Information Security Policies and all updates on the Company's intranet. The Human Resources Department shall provide each department and users without access to the intranet one printed copy of these policies at the same time the electronic version is published.

Management Responsibilities
- Management shall monitor all systems activity and network traffic to enforce the provisions of these policies.
- Management shall install access controls consistent with the requirements of these policies.
- Management and assigned administrators shall have the responsibility for testing access controls and the network for vulnerabilities.
- When vulnerabilities are known, users shall not exploit their effects by manual or programmatic means.
- Management and assigned administrators shall have access to the tools that can help manage and test information security.
Administrative Policy Cont’d.

Sample

Administrators' Responsibility

• Security, systems, and network administrators shall maintain records of all security violations.
• Security administrators shall maintain Risk Acceptance Memos for each waiver granted to these policies.
• Systems and network administrators shall be designated as the maintainers of user and access control information.
• Security, systems, and network administrators shall perform a semi-annual audit of user accounts and associated access controls to ensure validity and accuracy.
• Security, network, and systems administrators shall define the information that will be saved in systems and network logs.
• Authorized administrators shall review the system and other logs on a regular basis.
• Administrators shall take appropriate precautions to prevent logs from being deactivated, modified, or deleted.
• Administrators shall follow appropriate procedures when discovering violations of these policies or network security.
• Administrators shall backup active logs to an on-line storage facility. The on-line backup shall be archived to an off-line storage medium on the last day of each month. The off-line storage of logs shall be maintained for two years unless contract or the law requires longer periods.
Administrative Policy Cont’d.

Sample

Enforcement and Incident Reporting
• All users shall be responsible for maintaining and enforcing the provisions of these policies and associated procedures.
• Administrators shall monitor public disclosure organizations that report incidents, bugs, and other problems that could affect the security of the Company's network and systems.
• The response of violations from law enforcement shall be coordinated with management.
• Data regarding information security violations and incident handling shall be retained so that it may be used during the analysis of the information security policies.

Termination Policy
• Users whose association with the Company is terminated shall have their access privileges to the Company’s resources immediately revoked. Administrators shall arrange for the programs and other data used by these users archived. Administrators shall create procedures for revoking access of these users.
Any conduct which adversely affects the ability of others to use the company's systems and networks, or which can harm or offend others, shall not be permitted.

Management shall have the right to revoke any user's access privileges and terminate their association with the Company at any time for violations of this policy or demonstrates conduct that disrupts the normal operation of the Company's network and computing systems.

Management shall have the right to sever contracts and agreements with contractors and other outside users if they violate this policy or demonstrates conduct that disrupts the normal operation of the Company's network and computing systems.

Management shall have the right to exercise their options under the appropriate criminal and civil laws to seek legal remedies from anyone who uses, abuses, or attacks the Company's network and information systems in a manner that would be in violation of the law and these policies.