



## Customization of Information Security Policies & Procedures

Have You Updated Your Enterprise Policies Recently?

ecfirst has developed deep expertise in tailoring information security policies and procedures to meet compliance requirements and business priorities. Our impact on the customized development of your policies and procedures is typically based on:

- 1) In-depth understanding of regulatory requirements such as HIPAA but also many others including PCI DSS, Sarbanes-Oxley Section 404, as well as the ISO 27002 international security standard
- 2) Experience customizing hundreds of policies and procedures for organizations all across the United States
- 3) Hands-on experience working with information security projects in several areas including identity management, business continuity, vulnerability assessment including analysis of perimeter defense capabilities deployed
- 4) Our unique BizShield™ information security methodology that enables organizations to achieve complete compliance with regulatory requirements.
- 5) Our passion for ensuring complete client satisfaction for all work executed by us. We will not relent, unless we are assured that your organization is completely satisfied with the deliverables we have committed to.

### **OUR PROFESSIONAL TEAM**

The ecfirst team assigned to this engagement will only include credentialed professionals with deep experience developing information security policies and procedures for organizations. The intent is to leverage industry best practices so ensure that each policy genuinely reflects the actual process used within your organization and is influenced by regulatory requirements such as HIPAA, PCI DSS and others.

**SUMMARY OF POLICIES TYPICALLY DEVELOPED**

Figure 1 provides a brief summary of the objective of each security policy and procedure that organizations typically develop to address regulatory requirements. ecfirst will prepare the policies identified in Figure 1. ecfirst will review and enhance all existing policies. New policies will be developed if those do not exist in your organization.

Information Security Policy/Procedure	Description
<b>Administrative Safeguards Policies</b>	
Information Security Strategy	The purpose is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability (CIA) of information assets by protecting those assets from unauthorized access, modification, destruction, or disclosure.
<i>Security Management Process</i>	The purpose is to implement policies and procedures to prevent, detect, contain, and correct security violations.
Risk Analysis	The purpose is to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information.
Risk Management	The purpose is implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.
Sanction Policy	The purpose is to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the organization.
Information System Activity Review	The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

<i>Assigned Security Responsibility</i>	The purpose of this policy is to identify the security official who is responsible for the development and implementation of policies and procedures.
<i>Workforce Security</i>	The purpose is to implement policies and procedures to ensure that all members of the workforce have appropriate access to sensitive information and to prevent those workforce members who do not have access from obtaining access to sensitive information.
Authorization and/or Supervision	The purpose is to implement procedures for the authorization and/or supervision of workforce members who work with sensitive information or in locations where it might be accessed.
Workforce Clearance Procedure	The purpose is to implement procedures to determine that the access of a workforce member to sensitive information is appropriate.
Termination Procedures	The purpose is to implement procedures for terminating access to sensitive information when the employment of a workforce member ends.
<i>Information Access Management</i>	The purpose is to implement policies and procedures for authorizing access to sensitive information.
Access Authorization	The purpose is to implement policies and procedures for granting access to sensitive information, for example, authorization required to access a workstation, transaction, program, process, or other mechanism.
Access Establishment and Modification	The purpose is to implement policies and procedures that, based upon the

	entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
<i>Security Awareness and Training</i>	The purpose is to implement a security awareness and training program for all members of its workforce, including management.
Security Reminders	The purpose is to provide periodic security updates to all members of the workforce.
Protection from Malicious Software	The purpose is to develop procedures for guarding against, detecting, and reporting malicious software.
Log-in Monitoring	The purpose is to develop procedures for monitoring log-in attempts and reporting discrepancies.
Password Management	The purpose is to implement procedures for creating, changing and safeguarding passwords.
<i>Security Incident Procedures</i>	The purpose is to address security incidents.
Response and Reporting	The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
<i>Contingency Plan</i>	The purpose is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain sensitive information.

Data Backup Plan	The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information.
Disaster Recovery Plan	The purpose is to establish (and implement as needed) procedures to restore any loss of data.
Emergency Mode Operation Plan	The purpose is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in emergency mode.
Testing and Revision Procedures	The purpose is to implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis	The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components.
<i>Evaluation</i>	The purpose is to perform a technical and non-technical evaluation and subsequently, in response to environmental or operational changes affecting the security of sensitive information, that establishes the extent to which organization security policies and procedures meet the requirements of compliance requirements and business priorities.
<i>Business Associate Contracts and Other Arrangements</i>	The purpose is to obtain satisfactory assurances with impacted regulations that the business associate will appropriately safeguard all sensitive information.
<b>Physical Safeguards</b>	
<i>Facility Access Controls</i>	The purpose is to implement policies

	and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Contingency Operations	The purpose is to establish and implement as needed procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
Facility Security Plan	The purpose is to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Access Control and Validation Procedures	The purpose is to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
Maintenance Records	The purpose is to implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
<i>Workstation Use</i>	The purpose is to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access sensitive information.
<i>Workstation Security</i>	The purpose is to implement physical safeguards for all workstations that

	access sensitive information and restrict access to authorized users only.
<i>Device and Media Controls</i>	The purpose is to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, and the movement of these items within the facility.
Disposal	The purpose is to implement policies and procedures to address the final disposition of sensitive information, and/or the hardware or electronic media on which it is stored.
Media Re-use	The purpose is to implement procedures for removal of sensitive information from electronic media before the media are made available for re-use.
Accountability	The purpose is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Data Backup and Storage	The purpose is to create a retrievable, exact copy of sensitive information, when needed, before movement of equipment.
<b>Technical Safeguards</b>	
<i>Access Control</i>	The purpose is to implement technical policies and procedures for electronic information systems that maintain sensitive information to allow access only to those persons or software programs that have been granted access rights.
Unique User Identification	The purpose is to assign a unique

	name and/or number for identifying and tracking user identity.
Emergency Access Procedure	The purpose is to establish (and implement as needed) procedures for obtaining necessary sensitive information during an emergency.
Automatic Logoff	The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Encryption and Decryption	The purpose is to implement a mechanism to encrypt and decrypt sensitive information.
<i>Audit Controls</i>	The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.
<i>Integrity</i>	The purpose is to implement policies and procedures to protect sensitive information from improper alteration or destruction.
Mechanism to Authenticate Electronic Protected Health Information	The purpose is to implement electronic mechanisms to corroborate that sensitive information has not been altered or destroyed in an unauthorized manner.
<i>Person or Entity Authentication</i>	The purpose is to implement procedures to verify that a person or entity seeking access to sensitive information is the one claimed.
<i>Transmission Security</i>	The purpose is to implement technical security measures to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications

	network.
Integrity Controls	The purpose is to implement security measures to ensure that electronically transmitted sensitive information is not improperly modified without detection until disposed of.
Encryption	The purpose is to implement a mechanism to encrypt sensitive information whenever deemed appropriate.
<b>Organizational Framework</b>	
<i>Policies and Procedures Standard</i>	The purpose is to implement reasonable and appropriate policies and procedures to comply with applicable regulations.
<i>Documentation</i>	The purpose is to maintain the policies and procedures implemented to comply with regulations in written (or electronic) form and if an action, activity or assessment is required to maintain a written (which may be electronic) record.
<b>Other Policies</b>	
Information Classification	The Information Classification Policy is intended to assist employees of organization make decisions regarding what information may and may not be released to the public or disclosed to any individual outside of the organization.
Email Security	The purpose of this policy is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.
Remote Access Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to the organization's

	enterprise infrastructure to a reasonable and appropriate level.
Portable Devices Policy	The purpose is to secure the use of portable devices used by members of the workforce.
Wireless Security Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of organization's wireless infrastructure to a reasonable and appropriate level.

Figure 1: Summary of Information Security Policies and Procedures.

**OUR COMMITMENT TO YOU**

- 1) Closely examine all current information security policies and procedures.
- 2) Use ecfirst existing templates to tailor policies to your environment and format.
- 3) Update policies as required based on interviews and feedback provided to ecfirst.

**YOUR COMMITMENT TO US**

- 1) Copies of current policies and procedures needs to be provided for review and enhancement (if policies exist).
- 2) Feedback on template and draft must be received within 5 business days (or timeframe agreed to) of receipt from ecfirst.

**OUR DELIVERABLE TO YOU**

A complete set of customized policies all developed based on mutually agreed to requirements established at the start of the engagement.

**Fixed Fee with No Expenses:** Call for details and a customized proposal exclusively for your organization.

**COMPLIANCE PORTAL SITE LAUNCHED**

You are only 1-click away from major information security and business continuity related standards and key references at [www.ecfirst.com/complianceportal/](http://www.ecfirst.com/complianceportal/). Visit today.

**About ecfirst**

ecfirst delivers world-class information security, regulatory compliance solutions and its professional services team enables businesses address IT staffing challenges every day. With over 1400+ clients, ecfirst was recognized as an Inc. 500 business – America's Top 500 Fastest Growing Privately Held Business in 2004 – our first year of eligibility. ecfirst assists organizations with their compliance initiatives for a secure information infrastructure that is compliant with regulations such as PCI DSS, HIPAA,

Sarbanes-Oxley, ISO 27002, or federal and state legislations. ecfirst serves a Who's Who client list that includes technology firms, numerous hospitals, state and county governments, and hundreds of businesses across the United States and abroad. A partial list of clients includes EMC, IBM, Principal Financial, U.S. Army, U.S. Dept. of Homeland Security, U.S. Dept. of Veterans Affairs and many others.

### Information Security & Compliance

ecfirst delivers deep expertise with its full suite of services that include Single Sign-On (SSO), context management, contingency planning/Business Impact Analysis (BIA), vulnerability assessment, as well as managed compliance, security and IT infrastructure solutions. ecfirst has successfully executed fixed price, fixed deliverable, turnkey projects across the United States.

### World-class IT Professional Services

The ecfirst Professional Staffing Practice excels in meeting your short and long term requirements for contract professionals in the areas of Web development, system, database and network administration, application development, system architecture, and project management. This practice is distinguished with credentialed staff (PMP, CBCP, CISSP, CSCS, CHSS or others that may be required) that includes deep industry knowledge in the healthcare, financial, technology and government markets.

### Compliance and Training Certification

The ecfirst compliance training program is exclusively endorsed by the American Hospital Association (AHA). The Certified HIPAA Administrator (CHA<sup>TM</sup>), Certified HIPAA Professional (CHP) and the Certified HIPAA Security Specialist (CHSS<sup>TM</sup>) certifications are the gold standards in the Industry. The ecfirst Certified Security Compliance Specialist (CSCS) Program is the first and only information security program that addresses all major compliance regulations from a security perspective.

Talk to ecfirst.com and you will find an organization that is passionate about the services we deliver and exceptionally devoted to its clients. For more information, please visit <http://www.ecfirst.com/>.