
Legal Compliance with AirZip[®] FileSECURE[™]

Communicate with Confidence[™]

AirZip FileSECURE supports compliance with the Exploding Legal and Regulatory Mandates.

The dramatic increase in cybercrime, frequent cases of lack of internal corporate financial controls, and the recognized value of information to companies and individuals has resulted in the enactment of legislation and regulations requiring significant improvements in information protection. For example, many new laws require increased protection of financial information:

- Sarbanes-Oxley Act – Passed in 2002, this Act places strict requirements on company Boards and Officers to proactively prevent mishandling of information,
- Gramm-Leach-Bliley Financial Services Modernization Act - This US law passed in 1999 requires financial companies to protect non-public personal financial information (NPI) to prevent unauthorized disclosure and use.
- California SB 1386 (the California Information Security Act),
- New York Reg. 173 mandates the active encryption of sensitive financial information sent over the Internet.
- Homeland Security Information Sharing Act (HSISA, H.R. 4598), Security Rules and Regulations
- Healthcare Insurance Portability and Accessibility Act (HIPAA), place liability on anyone who fails to properly protect patient health information including bills and health related financial information.
- International Organization for Standardization (ISO) 17799, originally British Standard 7799. Defines an extensive approach to achieve information security including communications systems requirements for information handling and risk reduction,
- Basel Accord,
- European Union Data Protection Directive – Mandates protection of personal data,
- Japanese Protection for Personal Information Act, Kojin Joho Hogo HouA, May 2003,
- 17CFR Part 210's records retention,
- IASB's accounting procedures from AICPA and FASB,
- SEC and NASD, 21 CFR Part 11,
- NASB rules 2711 and 3010, and
- FDA 21 CFR-11.

Financial institutions, government agencies, healthcare organizations and professional services firms cannot meet current requirements with traditional firewall, VPN, and encryption solutions alone. These perimeter based methods cannot satisfy the requirements for improved information management and implementation of security policies of these laws and regulations.

AirZip FileSECURE implementation of Business Policies with a Positive Return on Investment

Business policies can generally be implemented manually or with adaptations to current systems. However, companies today are struggling with the high costs and low reliability of such implementations. Persistent Security, implemented with AirZip FileSECURE, creates a positive return on investment by reducing costs, increasing revenues, and avoiding losses in nine ways:

1. Avoided fines, penalties, and law suits due to improved monitoring of compliance with corporate policies, laws and regulatory requirements
2. Cost Reduction from lower administrative and management costs of complying with corporate policies, laws, and regulations due to improved monitoring of compliance with corporate policies, laws and regulatory requirements
3. Savings from improving protection of content integrity
4. Profit improvement due to improved protection of content royalties or direct impact of content on customer profits
5. Profit improvement due to new forms of business that would not be successful without persistent security functions
6. Avoided loss due to protecting intellectual property persistently everywhere every time
7. Avoided losses due to improved protection of content usage including ensuring use of the right content versions
8. Avoided losses due to monitoring content usage, distribution, and access
9. Avoided losses and costs due to improved enforcement of content life cycles by “shredding” old and unused files.

Compared to alternatives, AirZip FileSECURE does not add costs; it creates a positive return.

Why should you implement AirZip FileSECURE to support legal compliance?

Compliance with the information protection requirements of Title V, Section 5.01 of the Gramm—Leach—Bliley Act (GLB), the California State Senate Bill 1386, the Sarbanes Oxley Act, HIPAA, and many others is not optional. The security task is complicated since information not only must be protected in its home database, but also must be secured when in use. Information protection must exist within the institution and extend beyond the perimeter of the institution boundary to such entities as subcontractors. Recent losses of information by contractors have cost Well Fargo and UCSF many millions of dollars. AirZip FileSECURE can be used to insure excellent information security to avoid the pain that so many are experiencing.

AirZip FileSECURE provides many benefits including the following that support legal compliance:

- Protects information from the time it is acquired until it is purposely destroyed.
- Protects information that is transmitted to outside service providers.
- Tracks information use.
- Enhances efficient use of information rather than creating inefficiencies as a byproduct of security.
- Fits into current methods of information management and transmission.
- Is easy to install, use, and manage.

The remainder of this paper will provide examples of how AirZip FileSECURE supports compliance with particular laws. These examples illustrate the value for most of the laws listed above because the issues are similar in most of the laws and regulations.

California Senate Bill 1386

Compliance with the entire list of information protection laws and regulations listed above is supported by AirZip FileSECURE. A summary of California SB 1386 is given here along with a description of the value of AirZip FileSECURE in compliance. The "Personal Information: Privacy Act" was approved by the Governor September 25, 2002 and became effective July 1, 2003. It places new requirements on businesses that maintain computerized personal information on California residents. This law applies not only to businesses in California, but also to any business that conducts business in California whether or not the business has a physical presence in California.

The law requires that personal information must be protected.

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

BUSINESS REQUIREMENTS AND AIRZIP SOLUTIONS

Prevention of unauthorized disclosure is a business requirement. This requirement has many elements. AirZip FileSECURE provides the solution for each of these requirement elements.

BUSINESS REQUIRMENTS	AIRZIP FileSECURE SOLUTIONS
Protect personal information in primary data base from unauthorized access.	All files in a primary data base can be easily protected with AirZip FileSECURE. Individual files can be protected by the person who creates the file and then stores the file in the data base. Or FileSECURE can be configured with the data base to automatically protect every file that is stored in the data base with permissions unique to each individual directory. The files that are presented to a directory in the data base can be provided by people inside the organization or by customers or partners outside the organization with no special software on their computers. All of the files are then automatically protected from unauthorized access even when the files are copied out of the database to another storage media.
Allow different levels of access based on user need/authorization.	AirZIP FileSECURE allows different levels of access based on user need/authorization. FileSECURE enables a user to designate who will have permission to access information and set the level of permission. The user of FileSECURE can easily add, change or revoke permissions granted to file recipients. FileSECURE allows the system administrator to designate users, user groups, and establish security levels. The administrator defines security level categories and designates permissible activities within each category. The enterprise security administrator controls the list of those who are able to access, use, modify and share documents.

<p>Track information use and movement to support security monitoring.</p>	<p>AirZip FileSECURE tracks all uses of protected files meeting the requirements of SB 1386. AirZip FileSECURE provides comprehensive information usage reports, including the tracking of the following user and administrator actions:</p> <ul style="list-style-type: none"> • Account Activation, User Activation, User Updated, • User Deactivation, Login Accepted, Login Denied, • File Secured, File Secure Denied, File Viewed, • File Printed, File Saved Securely, • File Contents Copied, File Saved in Open, File Viewed, • File Permissions Changed, File Access Denied, • File Permissions Change Failure, • File Expire Date Set/Changed, File Owner Changed.
<p>Control access to and dissemination of information within the enterprise even when extracted from secure data base and moved to a non-secure environment online or to off line data storage.</p>	<p>AirZip FileSECURE is a flexible architecture for controlling access to and dissemination of information in non-secure environments online or offline. It uses the best existing products for encryption and authentication. AES256 is the encryption algorithm used in the standard product. However, other popular algorithms can be used if required by the customer. Customers have asked AirZip to utilize the customer's selected user authentication technology. So AirZip designed FileSECURE with the ability to integrate popular authentication solutions so that users can be recognized in the same way in all of the customer's applications.</p>
<p>Control access to and dissemination of information once it has been moved beyond the boundary of the enterprise (for example, to subcontractors).</p>	<p>AirZip FileSECURE is compatible with traditional firewall and VPN products and methods used to secure remote access to and from systems. In addition, implementation of AirZip FileSECURE enables necessary remote work functions to be performed without loss of control of information. Remote access to information is needed in most businesses. However, even when all of the traditional security methods for remote access are implemented, the information is able to be misused by the recipient upon receipt. But with FileSECURE, the use of that information can be restricted to block improper use by authorized people and eliminate access by unauthorized people.</p>
<p>Destroy copies of information once need for copies no longer exist, both within and beyond the enterprise boundary. (Note: this requirement is part of Civil Code Section 1798.81—not part of the Code added as a result of SB 1386.)</p>	<p>FileSECURE can specify time limits on access privileges granted to specific individuals. Access for specific time periods can be assigned to specific files, with access denied either before or after that period. Access Rights to a file can be terminated at any time. All protected copies of a file can be made non-accessible no matter where they are located.</p> <p>The elimination of a key to decrypt an AES 256 encrypted file can actually more effectively destroy copies of the file than erasing the file from digital media. Erasing all copies of files is often impossible because it is not possible to be certain where all of the copies are stored. Erasing a copy on most digital media requires overwriting the file 7 times with random bits. A single erase, the standard procedure, is not enough. Performing this type of erasing on some media, such as tapes, can damage the media causing other crucial information to be lost. If all copies of files are stored with view only permissions by FileSECURE, then access to all copies can be eliminated with total confidence.</p>

GRAMM—LEACH—BLILEY ACT

The Gramm—Leach—Bliley Act of 1999 states that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. The Act charges agencies with regulatory oversight responsibilities to establish appropriate standards for administrative, technical, and physical safeguards. The agencies have adopted "Guidelines Establishing Standards to Safeguard Customer Information". Banks were required to "...implement an information security program pursuant to these Guidelines by July 1, 2001". (Paragraph III.G.1) The agencies and the Federal Financial Institutions Examination Council have issued guidelines to support the examination and audit of the safeguards put in place by financial institutions. The regulations and the examination standards are the needs against which security tools can be measured. The subject of Title V of the Act is PRIVACY. Subtitle A (Sections 501—510), "Disclosure of Nonpublic Personal Information", places the obligation to protect nonpublic personal information on financial institutions.

BUSINESS REQUIREMENTS AND AIRZIP SOLUTIONS

Title V of the Gramm—Leach—Bliley Act requires financial institutions "...to protect the security and confidentiality of those customers' nonpublic personal information." (Section 501 (a)) To implement these provisions of the Act, the regulatory agencies (e.g., The Federal Reserve System) with oversight responsibilities for the financial services industry have issued a publication entitled "Interagency Guidelines for Establishing Standards For Safeguarding Customer Information". While the title contains the word "Guidelines" the mandatory nature of the requirements is clear from the content.

Together, the Interagency Guidelines and the IT Examination Handbook establish business requirements for financial institutions in the area of security of customers' nonpublic personal information. These business requirements are presented in the following table with the corresponding value of AirZip FileSECURE.

BUSINESS REQUIRMENTS	AIRZIP® FileSECURE Value
Logical and Administrative Access Control	
<p>Access Rights Administration</p> <p>Action Summary</p> <p>Financial institutions should have an effective process to administer access rights. The process should include the following controls:</p> <ul style="list-style-type: none"> • Assign users and system resources only the access required to perform their required functions, • Update access rights based on personnel or system changes, • Periodically review users' access rights at an appropriate frequency based on the risk to the application or system, and • Design appropriate acceptable-use policies and require users to sign them. (Page 15) 	<p>AirZip FileSECURE Author enables a user to designate who will have permission to access information controlled by the FileSECURE Author.</p> <p>The FileSECURE Author can easily add, change or revoke permissions granted to document recipients.</p> <p>FileSECURE Manager allows the system administrator to designate users, user groups, and establish security levels.</p> <p>The enterprise security administrator, as the user of FileSECURE Manager, controls the list of those who are able to use access, use, modify and share documents.</p> <p>FileSECURE Manager also allows the administrator to define security level categories and designate permissible activities within each category.</p>
1. New User Enrollment Process	FileSECURE Manager provides enrollment tools.

<p>2. Flexible Assignment Process, Based on:</p> <ul style="list-style-type: none"> a. Case by Case Accessibility to information b. Employee Role or Group Membership 	<p>FileSECURE Manager has an array of choices that enable the Security Administrator to assign information users to various categories, based on their particular needs or access and control permissions.</p>
<p>3. New User Enrollment Process</p>	<p>FileSECURE Manager provides enrollment tools.</p>
<p>4. Flexible Assignment Process, Based on:</p> <ul style="list-style-type: none"> a. Case by Case Accessibility to information b. Employee Role or Group Membership 	<p>FileSECURE Manager has an array of choices that enable the Security Administrator to assign information users to various categories, based on their particular needs or access and control permissions.</p>
<p>5. Tightly Controlled Privileged Access (i.e., Access Override Ability)</p>	<p>FileSECURE Manager puts the Security Administrator in control of assigning access and delegating limited access designation rights to trusted employees.</p>
<p>6. Access Rights Termination When Need No Longer Exists. (Automatic termination not anticipated by Guidelines; management process described.)</p>	<p>FileSECURE Manager can specify time limits on access privileges granted to specific individuals. Access for specific time periods can be assigned to specific documents, with access denied either before or after that period. Access Rights to a file can be terminated at any time by the Manager or Author.</p>
<p>Authentication</p> <p>Financial institutions should use effective authentication methods appropriate to the level of risk. Steps include</p> <ul style="list-style-type: none"> • Selecting authentication mechanisms based on the risk associated with the particular application or services; • Considering whether multi-factor authentication is appropriate for each application, taking into account that multifactor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities; and • Encrypting the transmission and storage of authenticators (e.g., passwords, PINs, digital certificates, and biometric templates). 	<p>AirZip FileSECURE uses strong but easy to deploy user authentication.</p> <ul style="list-style-type: none"> • Provides server based authentication – no complex certificate authority infrastructure. • Enables user to automatically authenticate with the server based on their Windows domain login. • Ensures that users are authorized to secure and use secured documents. • Its modular design permits incorporation of advanced authentication technologies such as card keys, thumb print scans, and others.

<p>Network Access</p> <p>Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access. Institutions should</p> <ul style="list-style-type: none"> • Group network servers, applications, data, and users into security domains (e.g., untrusted external networks, external service providers, or various internal user systems); • Establish appropriate access requirements within and between each security domain; and • Implement appropriate technological controls to meet those access requirements consistently. 	<p>AirZip FileSECURE is compatible with products used to protect computer networks. Such protection of computer networks is helpful but is made less significant by the fact that AirZip FileSECURE protects the information itself.</p> <p>An organization that depends on access controls to protect information is like an army that depends on a fort for protection. A fort is not effective in the modern military because enemies can penetrate any fixed location fort. The same is true of today's computer networks in that they can be penetrated and information can not be kept inside. Files must be protected, not just the network.</p>
<p>Operating System Access</p> <p>Financial institutions should secure access to the operating systems of all system components by</p> <ul style="list-style-type: none"> • Securing access to system utilities, • Restricting and monitoring privileged access, • Logging and monitoring user or program access to sensitive resources and alerting on security events, • Updating the operating system with security patches, and • Securing the devices that can access the operating system through physical and logical means. 	<p>AirZip FileSECURE is compatible with products and methods used to secure access to operating systems.</p>
<p>Application Access</p> <p>Financial institutions should control access to applications by</p> <ul style="list-style-type: none"> • Using authentication and authorization controls appropriately robust for the risk of the application, • Monitoring access rights to ensure they are the minimum required for the user's current business needs, • Using time of day limitations on access as appropriate, • Logging access and security events, and • Using software that enables rapid analysis of user activities. 	<p>AirZip FileSECURE is compatible with products and methods used to control access to applications.</p>
<p>Physical Security</p> <p>Financial institutions should define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of</p> <ul style="list-style-type: none"> • Physical penetration by malicious or unauthorized people, • Damage from environmental contaminants, and • Electronic penetration through active or passive electronic emissions. (Page 44) 	<p>AirZip FileSECURE is compatible with products and methods used for physical security.</p>

<p>Encryption</p> <p>Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit. Encryption implementation should include</p> <ul style="list-style-type: none"> • Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk, • Effective key management practices, • Robust reliability, and • Appropriate protection of the encrypted communication's endpoints. (Page 48) 	<p>AirZip FileSECURE is a flexible architecture for persistent security and tracking. It uses the best existing products for encryption and authentication. AES256 is the encryption algorithm used in the standard product. Other algorithms can be integrated.</p>
<p>Remote Access</p> <p>Financial institutions should secure remote access to and from their systems by</p> <ul style="list-style-type: none"> • Disabling remote communications at the operating system level if no business need exists, • Tightly controlling access through management approvals and subsequent audits, • Implementing robust controls over configuration to disallow potential malicious use, • Logging and monitoring remote access, • Securing remote access devices, and • Using strong authentication and encryption to secure communications. (Page 43) 	<p>AirZip FileSECURE is compatible with products and methods used to secure remote access to and from systems. In addition, implementation of AirZip FileSECURE enables necessary remote work functions to be performed without loss of control of information. Remote access to information is needed in most businesses. However, even when all of the security requirements described to the left for remote access are implemented, the information is able to be misused by the recipient. But with FileSECURE, the use of that information can be restricted and tracked reduce the opportunities for misuse.</p>
<p>Malicious Code</p> <p>Financial institutions should protect against the risk of malicious code by</p> <ul style="list-style-type: none"> • Using anti-virus products on clients and servers; • Using an appropriate blocking strategy on the network perimeter; • Filtering input to applications; and • Creating, implementing, and training staff in appropriate computing policies and practices. (Page 53) 	<p>AirZip FileSECURE is compatible with products and methods used to block malicious code. In certain cases, some adjustments are required to allow malicious code blockers to recognize AirZip protected files.</p>
<p>Systems Development, Acquisition, and Maintenance</p> <p>Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include</p> <ul style="list-style-type: none"> • Defining security requirements before developing or acquiring new systems; • Incorporating widely recognized standards in developing security requirements; • Incorporating appropriate security controls, audit trails, and logs for data entry and data processing; • Implementing an effective change control process; • Hardening systems before deployment; • Establishing an effective patch process for new security vulnerabilities; and • Overseeing vendors to protect the integrity and confidentiality of application source code. (Page 55) 	<p>Although this section focuses on new systems and application software, the AirZip™ suite of security tools are easily applied to existing systems and could easily be used with new software applications if this were specified by the financial institution. Indeed, because AirZip™ tools are designed to provide persistent security and are easy to install and use, they become an attractive specification for the financial institution to identify when developing, acquiring, or commissioning development of new software applications.</p>

<p>Personnel Security</p> <p>Financial institutions should mitigate the risks posed by internal users by</p> <ul style="list-style-type: none"> • Performing appropriate background checks and screening of new employees; • Obtaining agreements covering confidentiality, nondisclosure, and authorized use; • Using job descriptions, employment agreements and training to increase accountability for security; and • Providing training to support awareness and policy compliance. 	<p>AirZip FileSECURE mitigates the risks posed by internal users by providing the tools necessary to customize access permissions to only the level required by the individual users.</p>
<p>Electronic and Paper-Based Media Handling</p> <p>Financial Institutions should control and protect access to paper, film and computer-based media to avoid loss or damage. Institutions should</p> <ul style="list-style-type: none"> • Establish and ensure compliance with policies for handling and storing information, • Ensure safe and secure disposal of sensitive media, and • Secure media in transit or transmission to third parties. (Page 62) <p>This section deals with the physical security of media. The emphasis is on the physical storage, physical destruction after use, and physical protection while in transit. However, in the discussion on storage, the point is made that (m)anagement should establish access controls to limit access to media, while ensuring all employees have authorization to access the minimum level of data required to perform their responsibilities.</p>	<p>AirZip FileSECURE provides all the tools necessary to protect digitally based information. This includes protecting information from unauthorized access in its primary location, while in transit, and while used by authorized recipients. FileSECURE can also be used to dispose of digitally based information.</p> <p>In addition, AirZip FileSECURE enables organizations to protect image files produced by scanning paper files. This permits secure communications of images of documents instead of poorly secured transmission and handling of FAX copies.</p>
<p>Logging and Data Collection</p> <p>Financial institutions should</p> <ul style="list-style-type: none"> • Identify the system components that warrant logging, • Determine the level of data logged for each component, and • Establish policies for securely handling and analyzing the log files.(Page 64) <p>The following data are typically logged to some extent including</p> <ul style="list-style-type: none"> • Inbound and outbound internet traffic • Internal network traffic, • Application access 	<p>AirZip FileSECURE provides comprehensive information usage reports, including the tracking of many user and administrator actions.</p>
<p>Service Provider Oversight</p> <p>Financial institutions should exercise their security responsibilities for outsourced operations through</p> <ul style="list-style-type: none"> • Appropriate due diligence in service provider research and selection; • Contractual assurances regarding security responsibilities, controls, and reporting; • Nondisclosure agreements regarding the institution's systems and data; • Third-party review of the service provider's security through appropriate audits and tests; and • Coordination of incident response policies and contractual notification requirements. 	<p>AirZip FileSECURE enables information security consistent with that required within the boundaries of the enterprise to extend to service providers employed by the financial institution. Any secure information transmitted to a service provider can be protected even after transmission and its use tightly controlled. Access to transmitted information can be enabled for a period of time and then disabled once the service provider no longer has a need for the information. All uses of the information can be recorded and access denied if usage patterns are not normal.</p>

<p>Intrusion Detection and Response</p> <p>Financial institutions should have the capability to detect and respond to an information system intrusion commensurate with risk. Risk mitigation practices include</p> <ul style="list-style-type: none"> • Preparation, including analysis of data flows, decisions on the nature and scope of monitoring, consideration of legal factors, appropriate policies governing detection and response, and formation and equipping of response teams; • Detection implementation, including the proper use of technology; and • Response to an intrusion, including the containment and restoration of systems and appropriate reporting. 	<p>Since AirZip FileSECURE tracks all access to protected information, abnormal usage patterns can be detected. Actions can be automatically taken upon the occurrence of certain events or sequences of events. And the data can support investigations of the causes of abnormalities.</p>
<p>Business Continuity Considerations</p> <p>Financial institutions should consider</p> <ul style="list-style-type: none"> • Identification of personnel with key security roles during a continuity plan implementation, and training personnel in those roles; and • Security needs for back-up sites and alternate communication networks. 	<p>AirZip FileSECURE insures file recovery is possible in the event of server system failure by providing the account owner with a “master key” pair.</p>
<p>Insurance</p> <p>Financial institutions should carefully evaluate the extent and availability of coverage in relation to the specific risks they are seeking to mitigate.</p>	<p>AirZip FileSECURE can be shown to reduce risks.</p>

About AirZip

AirZip is the leader in controlled content protection and electronic file distribution for the enterprise.

AirZip is a wholly owned subsidiary of Willow Technology, a leading enterprise middleware provider.

Contact information:

AirZip, Inc,
469 El Camino Real, Suite 220
Santa Clara, CA 95050
USA
phone: +1.408.247.3820
email: info@airzip.com
www.airzip.com

©Copyright 2002-2006 AirZip, Inc. All Rights Reserved.
AirZip is a registered trademark AutoSECURE, DiskSECURE, FileSECURE, MailSECURE and ScanSECURE are trademarks of AirZip, Inc. in the United States and other countries.
Specifications subject to change.