AirZip® FileSECURE™ White Paper

Communicate with Confidence™

Introduction

Keeping personal or sensitive information confidential is an essential aspect when doing business today. The disclosure of confidential information whether it happens intentionally or accidentally often damages a corporation's reputation and business. Moreover, accidentally disclosing confidential information can also harm the information owner since any incident may lead to unpredictable consequences, which could translate at best into embarrassment and, in the last resort, into job loss.

AirZip FileSECURE is a very powerful yet easy to use Enterprise Rights Management application for sharing confidential and sensitive information without giving up control. It enables the owner of information to determine who can access information, how and when it can be used, and to record all uses of the information. AirZip FileSECURE is built to integrate with current systems. Thus, the information owner can *communicate with confidence* knowing that the information will be used only as permitted.

Confidentiality in a Business Environment

Confidentiality has been defined by the International Standards Organization (ISO) as "ensuring that information is accessible only to those authorized to have access." Every business has to deal with a variety of sensitive information that has to be kept confidential in order to stay competitive and to comply with information management policies, laws, and regulations. Therefore, every individual working for an organization is obliged to keep sensitive information confidential within his or her area of accountability. For instance, with digital files, it is very easy for well intended people, to make a mistake that puts confidential information into the wrong hands. The email "reply to all" command is a powerful tool for disclosing information that should kept confidential. Very often, the "reply to all" command is used without thoroughly checking the entire distribution list. Attaching a confidential file and using the "reply to all" command when the address list includes a recipient that is not authorized to access the file, causes loss that is often never noticed.

Examples of information that businesses should keep confidential:

- Employee's personal information in human resources
- Executive communications – among themselves, to subordinates and to board members
- Intellectual property in engineering and R&D
- Customer lists and pricing information in marketing
- Financial statements that are not yet published in finance
- Negotiated contracts in legal

Every organization and also every employee should be aware of the importance of confidentiality when doing business. Reasons for the importance include:

To avoid high cost due to disclosure of confidential information

Disclosure of confidential information often translates into high cost because of the loss of valuable intellectual property. Many companies are reporting significant information value loss. Security executives are most concerned about fraud and even inadvertent disclosure by employees (Employees, 55%; Hackers, 38%; Partners, 8%) (USA Today 2/4/'03). A PriceWaterhouseCoopers study stated that "70 percent or more of the market value of a typical US company resides in intellectual property (IP) assets." And the following chart shows that most companies experience loss of these assets:

High Cost of Information Loss	$K/ Incident	% Companies
R&D	404	49
Financial data	356	27
2nd party information	165	4
Customer lists	117	36
Strategic plans	20	25
M&A	20	16
Manufacturing data	20	16

Network Computing Magazine; January 2003

A 2003 Federal Trade Commission survey estimated that nearly 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated $48 billion in losses, and costing consumers an additional $5 billion in out-of-pocket losses. (*Identity Theft Survey Report* (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

To protect a company's reputation, brand image and business relationships

Disclosure of confidential information such as customer lists or 2nd party information can lead to a substantial damage of a company's reputation, its brand image, and existing business relationships. A lot of companies have experienced the consequences of disclosing sensitive information in recent years. Numerous companies have paid hefty fines to the Federal Trade Commission (FTC) in recent years, as well as suffering significant brand damage. (http://www.FTC.gov/privacy).

To comply with legal and regulatory mandates

- 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, July 2002;
- Japanese Protection for Personal Information Act, Kojin Joho Hogo HouA, April 2005;
- 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;
- FDA 21 CFR-11.

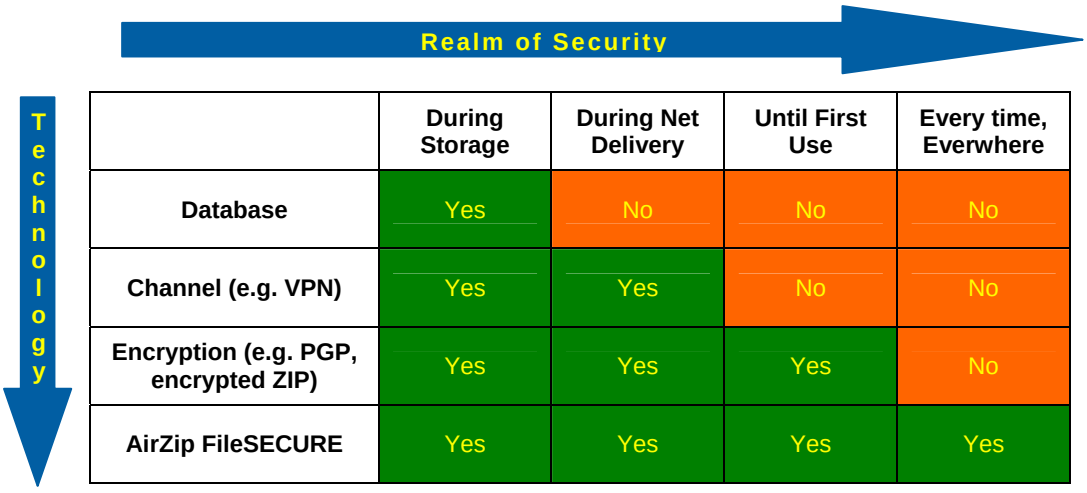
How AirZip FileSECURE helps to keep information confidential

AirZip FileSECURE reduces the risk of intellectual property loss, speeds business processes, and reduces administrative costs while at the same time helping to meet legal, regulatory and other information management requirements.

AirZip FileSECURE enables information owners to *communicate with confidence* by performing the following functions:

- **Securing** sensitive documents from cradle to grave.
- **Tracking** all usage, providing legal evidence of who has actually viewed which documents.
- **Controlling** by allowing dynamic changes to permissions, enabling complete control of sensitive information all the time.
- **Accelerating** communications by compressing the content before encryption.

AirZip FileSECURE protects files consistently and constantly ensuring loss prevention, version control, time based availability and retention management.



	During Storage	During Net Delivery	Until First Use	Every time, Everwhere
Database	Yes	No	No	No
Channel (e.g. VPN)	Yes	Yes	No	No
Encryption (e.g. PGP, encrypted ZIP)	Yes	Yes	Yes	No
AirZip FileSECURE	Yes	Yes	Yes	Yes

The AirZip FileSECURE Reader also protects against viruses and worms by blocking the execution of any executable files that might be attached to the protected file. Thus, you can open an AirZip FileSECURE protected file with confidence that doing so will not result in contamination of your computer with a virus.

AirZip FileSECURE is configured using five key components:

1. FileSECURE **Author** – enables users to persistently secure confidential documents, email secured documents to internal or external users, modify or revoke document permissions.
2. FileSECURE **Editor** – enables users to view or edit secured Microsoft Office documents.
3. FileSECURE **Reader** – enables users to view or use secured documents.
4. FileSECURE **Manager** – enables administrator to rapidly define users, user groups, categories and category permission (policies).
5. FileSECURE **Authentication & Policy Server** – stores all user and file usage information with a minimum of system administration (may be deployed on any Windows, Mac OS X, Unix, or Linux computer).

AirZip FileSECURE Author - simplifies protecting confidential information

Users will find the AirZip FileSECURE client interface to be easy and intuitive to use. Keeping information confidential is as easy as clicking the Secure icon (or right clicking a file in Windows Explorer) and selecting permissions. Then the file can be stored and transmitted in any manner using the standard tools used by the user every day.

AirZip FileSECURE client is a Windows application that simplifies the securing of any confidential information by enabling users to

- Locate and secure any file.
- View and use secured files that they are authorized to use.
- Email secured files in seconds in a manner compatible with popular email clients.
- Add users to whom confidential information must be communicated.
- Determine what has happened to each secured file and
- Change permissions at any time.

Users of AirZip FileSECURE can select from the following permissions:

- View – Allows viewing of the document.
- Print – Allows printing of hard copies.
- Copy – Allows user to select and copy portions of the file (or the entire file) to the clipboard or to save unencrypted copies of files.
- Control – Allows user to change permission assignment or to revoke all permissions.
- Available starting time – Allows users to safely send a file before the file is available for use.
- Expires after – Allows users to revoke permission after a specific amount of time.

FileSECURE will control 'Availability' and 'Expiration' times to the granularity of a minute. Time selection is based on Server time to avoid inaccuracies of client time settings. For example, if a user specifies that permission to use a file shall expire at 2:00pm on Wednesday August 23rd, 2004, the file will be unavailable at that time as determined by the server.

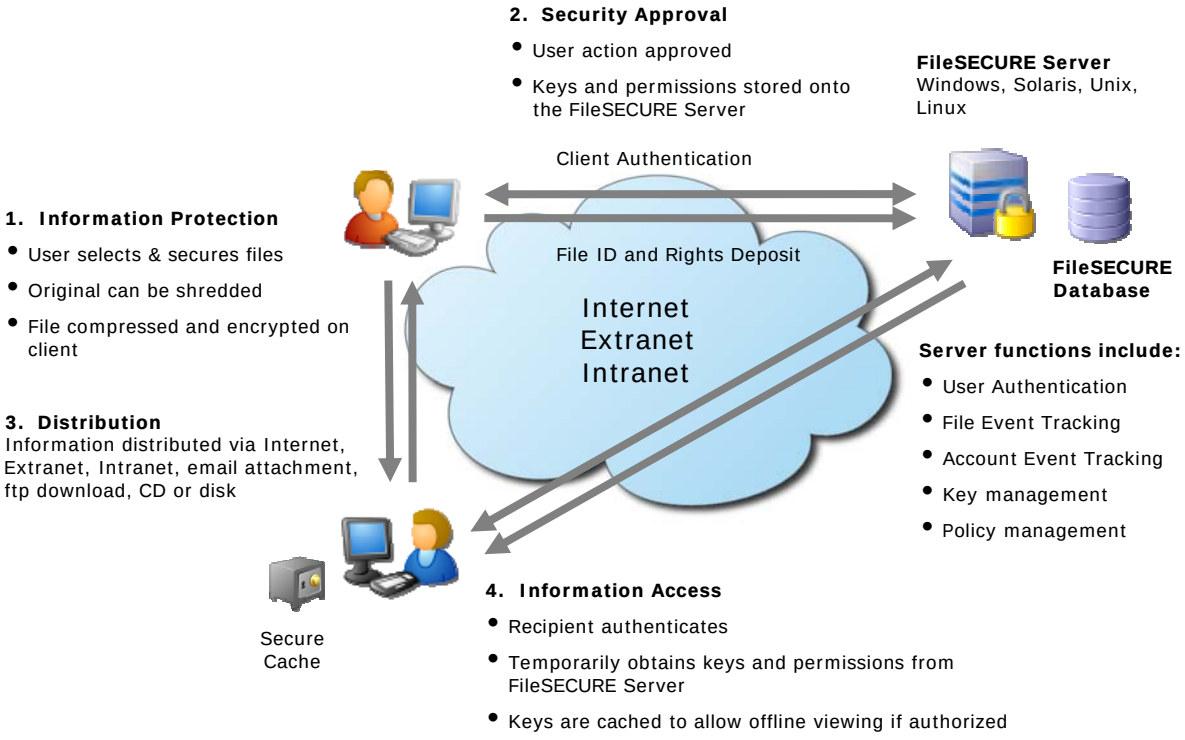
AirZip FileSECURE Reader - simplifies use of secured confidential information

AirZip FileSECURE Reader is an easily downloaded application that can also be launched as a Windows Active X control within Internet Explorer. It is easier to download than a PDF reader and enables fast viewing of secured documents. The Reader allows users to:

- Open secured confidential files even without the original application installed on their computer.
- Display available permissions.
- Save secured files.
- Print secured files if allowed.
- Copy content from a secured file if allowed.

Adapting to and streamlining current work flow

AirZip FileSECURE enables persistent security to fit into current work flow patterns by enabling confidential files to be protected at the point of creation of the information; the author's personal computer. The following chart describes the AirZip FileSECURE architecture for this application:



With this configuration, AirZip FileSECURE enables a user to protect confidential files stored on user's hard drive, server drive, or shared on web sites and send the protected file to anyone using e-mail, file download from a server, CD-ROM, or any other method.

AirZip FileSECURE can also be configured to dynamically and automatically protect confidential files at the time they are stored in any selected directory. All files stored in selected document directories are automatically protected. Files are protected with no change in the user's actions and no new software on the personal computer of the originating party. This configuration can be very powerful in applications where many customers want to provide sensitive information to an organization and maintain control over the use of that information. Laws require that healthcare and personal financial information be used in ways that the owner of that information approves. By using this architecture, personal financial information could be provided by an individual to several banks for loan approval. The individual could specify who is permitted to view the information for evaluation. When the individual decides from which bank to get a loan, the individual would be able to prevent the disclosure of his/her information to the other organizations. And this can be implemented with no special software on the computer of the individual.

Strong encryption to protect confidential files

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. For customers in the Peoples Republic of China, AirZip offers Chinese government approved SSF08 encryption using USB connected devices.

Benefits of keeping Information confidential with AirZip FileSECURE

Protecting any Type of File

- Protection of any file that should be kept confidential.
- Protected viewing of any file that can be printed.
- Blocking of electronic screen image capture.
- Extracting the original file, if permitted, from the protected file.

Strong Encryption without Key Management

- Securing a file by clicking Secure and selecting permissions.
- AES 256 bit encryption (SSF08 for Peoples Republic of China customers).
- Only the email address of intended user required to provide file access.

Persistent Access Protection

- Insurance that confidential information is protected wherever it is stored or transmitted, not just when in transit.
- Insurance that only authorized recipients can access confidential files, and only at the times specified, no matter where the recipient is located - both on or off-line.
- Enabling file owners to dynamically change user permissions even after the file has been distributed.
- Enforcement of file retention policies to insure that old information is not accessible.

Efficient Distribution and Version Control

- Distribution of confidential files with the assurance that only authorized recipients have viewing ability, eliminating risks in internal and external communications.
- Protected files can be shared using any method - email, CD-ROM, FTP download, etc.
- When a new version is available for distribution, the viewing permission of the old version of the file is revoked.
- Keeping track of who has viewed or not viewed a confidential file, to meet regulatory or legal compliance.
- Working with users' default email software to easily send protected attachments.
- Accelerating by compressing the content before transmission.

Intuitive User Interfaces

- Securing confidential documents directly from within Windows Explorer and Microsoft Office applications.
- Using AirZip FileSECURE Author interface to secure folders or entire disk drives is easy.

Simple Administration

- Easy adding, editing and disabling of individual users.
- Adding new reader in seconds without involvement of an administrator.
- Reader software is relatively small; thus, easy and fast to download.
- Only authorized users may open secure files.

Easily understood Permission Controls

- View – Allows viewing.
- Print – Allows printing.
- Copy/Save – Allows copy or save unencrypted copies.
- Control – Allows user to change permissions.
- Start Time - Allows users to send a file before the file is available for use.
- Expire Time - Allows revocation of permissions at a time or after an interval.

Comprehensive Audit Trail

- Creating an audit trail tracking all actions including file access, viewing, denial of access, and all administrative events
- Providing proof of compliance with your organization's information security policies.

Integration with Corporate Directory and Authentication Infrastructure

- Synchronizing user accounts and group definitions with IBM Directory Server, IBM Secureway Directory Server, Lotus Domino, Microsoft Active Directory, Novell eDirectory/NDS, Sun One Directory Server 5.2 or Tivoli Directory Server.
- Reducing and isolating administration efforts.

Ease of Use and Deployment

- Possibility to send one file to many users with unique permissions for each person.
- Compliance with laws, regulations, and corporate policies.
- Cross platform server deployment: Apple Mac OS X, HP-UX, IBM AIX, Linux, Microsoft Windows, SGI Altix, Sun Solaris, UnixWare.

Summary

If companies want to stay competitive they will have to deal with the issue of how to protect their confidential information in an easy and effective way. AirZip FileSECURE is an easy and convenient application to prevent the disclosure of confidential information. Besides its various functional benefits such as the protection of any type of file and strong encryption, it is easy to implement and use. Thus, a business will not need a lot of time to train its employees, but it will be able to reduce the risk of disclosing sensitive information fast and effectively after implementing AirZip FileSECURE. Accordingly, having implemented AirZip FileSECURE, a company will also comply with legal and regulatory mandates a decrease the risk of reputation damage associated with the disclosure of confidential information.

AirZip FileSECURE VALUE CREATION SUMMARY

The persistent protection of confidential information, tracking and document retention management capabilities of AirZip FileSECURE enable you to communicate with confidence that your valuable information is protected.

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 software provider.

Contact information:

AirZip, Inc,
961 Red Tail Lane
Bellingham, WA 98226
USA
phone: +1.360.922.0613
email: info@airzip.com
www.airzip.com