



Go

Public CIO Home

Latest CIO News
 Advice & Opinion
 Case Studies & Interviews
 Enterprise Technology
 IT Management & Governance
 Leadership Strategies & Careers
 Research

Get PCIO News Via Email**Industry Perspectives**

Case Studies
 White Papers
 Partner Sites

Public CIO Magazine

Current Issue
 Subscribe
 Contact
 Contribute

Simplifying Information Security



Aug 16, 2010, By **Terry Wieczorek**

Advanced digital technology makes document creation, usage and storage quicker and easier than ever before. But the very fact that digital

documents can be easily copied, stored and transmitted through multiple communication channels raises obvious security questions. Federal, state and local governments -- as well as the private organizations that work with them -- regularly collect and store private, personal and sensitive information, including military or police intelligence and municipal archives of birth certificates. It is imperative that these agencies can quickly and efficiently receive and distribute this information safely to the public and authorized individuals.

And with today's multiple communication avenues -- including wired and mobile phones, and the Internet and its video streaming -- the chances for unauthorized access to data archives are at an all-time high. This access can be difficult to detect and ultimately may result in missing or altered documents, which can be costly and involve damaging liabilities for agencies and citizens.

By carefully assessing your agency's information access and security demands, you can take the steps necessary to build and create an effective document archive and retrieval system. With the help of the right solutions, protecting an individual's information has never been easier.

Creating the Plan

Developing an effective, efficient and secure data archive system begins with a review of applicable regulations or public policies, and then assessing your agency or location's specific needs and requirements. To create a solid foundation for a suitable digital archive system, every security policy must address all legal requirements and public concerns. The federal government's National Institute of Standards and Technology (NIST) offers a plethora of studies and guidelines for handling digital information and documents, and these standards can vary widely depending upon how government agencies and even private industries collect and use this information.

NIST's Computer Security Division has published the booklet Minimum Security Requirements for Federal Information and Information Systems, reference number FIPS 200 (Federal Information Processing Standards 200), that identifies three key issues as a starting place for developing an effective and practical security policy: confidentiality, integrity and availability.

Confidentiality

Protecting data confidentiality is absolutely essential in many situations. Military intelligence is one example and transportation-related information is another. Detailed floor plans for airports and other transportation terminals often are kept confidential, as are plans and routes for moving or storing certain types of products or materials. Medical information is protected by Health Insurance Portability and Accountability Act (HIPAA) regulations, and personal information on citizens and government employees also should be kept confidential or granted only to authorized individuals.

SHARE

Comment

Related Products

We help state and local governments connect to citizens with our services, learn more here. : Pitney Bowes Business Insight
 Increase performance and lower your costs with EMC unified storage. : EMC

Tools Sponsored By**Get Public CIO's Bi-Weekly Newsletter**

Email: [view sample](#)

Video

**Warning to Vendors**

Vendors charging high maintenance fees are put on notice to cut their rates by Steve Emanuel, CIO of Montgomery County, Md.

**Virtual Beverly Hills 1**

Spanning earthquakes to water meters, Beverly Hills rolled out an interactive and interoperable Web-based GIS portal for emergency operations and public information.

**Virtual Beverly Hills 2**

Virtual Beverly Hills was recently challenged when a crowd of more than 20,000 ran through town.

[More Video >](#)

Government Jobs

Browse hundreds of public sector career opportunities in GovTech's new jobs section. Popular job searches: **government IT, public safety, GIS, transportation, CIO, security, health**



Mobile Public Safety Communications at Blazing-Fast Speeds

Click here to view our robust online arsenal of case studies, research and resources. >>>





Integrity

Data integrity is necessary in every situation. That is, the information in a document should be stored in its true fidelity, and it should be tamper-proof or at least leave some indication that it has been changed, corrected or updated, when this was done and by whom.

Availability

Though availability would seem contradictory to confidentiality, much of the information that government agencies collect, such as local rainfall totals or population demographics, is intended for public distribution. Availability also covers "need-to-know" issues, like who in the agency is authorized to access certain stored data daily, or who may require immediate access to certain documents and information in an emergency.

Devising a secure archive solution to meet a government organization's complex issues and needs means more than just buying a solution in a box. It requires a team effort to develop procedures that bridge the gap between your specific agency or location and the general standards created by broader governmental policies.

Once the policy is implemented, "eternal vigilance" becomes the order of the day. The agency and staff must make a genuine commitment to finding and deploying the best hardware and software to support the level of security your data archive requires,

1 | **2** Next >

0

tweets

tweet

➤ Latest Government Technology News

Northrop Grumman Vows to Find Cause of Virginia Server Meltdown as Fix Nears - Sep 1

Wisconsin Bans Trashing of Electronics - Sep 1

Amazon Kindles Connect Rural Libraries to Digital World - Aug 31

Economy Forces County IT Departments to Embrace Practicality - Aug 31

Briefs: McKinney, Texas, Hires Former Colorado Springs IT Manager - Aug 31

[View All Government Technology News](#)

➤ Industry Solutions for Government

Read real world deployments of technology in government from our sponsors.

Cyber Security Cases

Economic Development Cases

Enterprise Cases

[View All Industry Solutions](#)

➤ Marketplace

SAS earns top ranking in predictive analytics and data mining. Read report.

Read this four-part series on realizing a more accountable government.

See how Adobe opens up government

Road Map to the Virtual Data Center – Journey to the Private Cloud

➤ Related Products and Services

Take full advantage of wireless & mobile technologies with HP Care Pack Smart Support services : Hewlett-Packard

Ensure device & data security as well as reliable connectivity with Security &





Go

Public CIO Home

[Latest CIO News](#)
[Advice & Opinion](#)
[Case Studies & Interviews](#)
[Enterprise Technology](#)
[IT Management & Governance](#)
[Leadership Strategies & Careers](#)
[Research](#)
Get PCIO News Via Email
Industry Perspectives
[Case Studies](#)
[White Papers](#)
[Partner Sites](#)
Public CIO Magazine
[Current Issue](#)
[Subscribe](#)
[Contact](#)
[Contribute](#)

Simplifying Information Security

Aug 16, 2010, By **Terry Wiczorek**

(Page 2 of 2)

and constant maintenance and upgrading of these systems is important.

The Art of Building the System

Once you've determined your exact archive security needs and requirements that must be met, the real work begins. It's important to take into account three aspects that encompass archiving security: physical security, network security and data security. Let's take a look:

Physical Security. This involves allowing only authorized and authenticated personnel to access the archive system, and then to access only those documents they need to perform their jobs. Authorized access should include an audit trail for all record transactions; protect physical records and media; support distributed management of records; provide for conversion and migration of records; allow users to access, retrieve and use records; and facilitate records retention and disposition throughout the document life cycle. These rules must be designed for all documents, yet be flexible enough to suit different document types and meet all current and future compliance regulations.

Network Security. Common solutions for network security include firewalls and data management zones (DMZ). Firewalls can include both hardware and software, and provide a filtering mechanism that examines incoming/outgoing data and allows only authorized data to pass through. DMZs basically are subnetworks that stand between an organization's most secure internal network and the outside world. A DMZ might include devices like Web servers, mail servers, file transfer protocol servers and VoIP servers that communicate directly -- or through a firewall -- with the Internet. Any incoming data passed beyond the DMZ into the internal network should be scrutinized by a second, more restrictive firewall.

Data Security. All archived data stored on a server should be protected by physical and network safeguards, or they can be stored on CDs or other removable storage devices in a physically secure, limited-access facility. CDs also can be password protected and the data encrypted and compressed for even further protection. In either case, the document must be readable, perhaps even years after it was created. The PDF offers both space-saving file compression and platform independence, allowing documents to be viewed on the desktop.

The Human Factor Weighs In

Despite the fact that so much data is automated today, always remember that people create and manage document archiving systems, and people also retain and distribute these documents. Information integrity is essential to helping people make appropriate decisions based on the data, so information must be retrieved quickly and as easily as possible to satisfy the public's needs. It also must rapidly be available to those needing it during a crisis or emergency.

The most important part of a secure document archive system is trustworthy personnel and ensuring that they understand your organization's document security goals and the importance of their positions. Not only does everyone working with the archive system need to be trained in its operation, they also must understand the need for security and take the issue seriously. All staff members who can access and distribute archived information must be updated on both internal and governmental policy, as well as

SHARE

Comment

Related Products

Take full advantage of wireless & mobile technologies with HP Care Pack Smart Support services : Hewlett-Packard

Ensure device & data security as well as reliable connectivity with Security & Management Solutions : Hewlett-Packard

Tools Sponsored By

Get Public CIO's Bi-Weekly Newsletter

Email:

Go [view sample](#)

Video



Warning to Vendors

Vendors charging high maintenance fees are put on notice to cut their rates by Steve Emanuel, CIO of Montgomery County, Md.



Virtual Beverly Hills 1

Spanning earthquakes to water meters, Beverly Hills rolled out an interactive and interoperable Web-based GIS portal for emergency operations and public information.



Virtual Beverly Hills 2

Virtual Beverly Hills was recently challenged when a crowd of more than 20,000 ran through town.

[More Video >](#)

Government Jobs

Browse hundreds of public sector career opportunities in GovTech's new jobs section. Popular job searches: **government IT, public safety, GIS, transportation, CIO, security, health**



Mobile Public Safety Communications at Blazing-Fast Speeds

Click here to view our robust online arsenal of case studies, research and resources. >>>





technology upgrades and operational changes. Like the archived data itself, these changes should be monitored and recorded regularly.

Summing it Up

Our society is increasingly being run on the basis of information. Think of the number and types of permits, licenses, birth and marriage certificates, legal and court documents stored by government agencies, and how citizens and government staff use these relatively common documents daily. While new technologies would appear to put these documents at greater risk, the security challenges they pose are being solved by even more sophisticated technology solutions. Once you have a solid understanding of your location's need for information access and security, you can implement a safe, practical and affordable document archive and retrieval system.

Terry Wieczorek is president and CEO of DocuLynx Inc., a provider of archive retrieval, electronic distribution and Web presentment solutions for print service providers.

MJ

1 | 2



Latest Government Technology News

Northrop Grumman Vows to Find Cause of Virginia Server Meltdown as Fix Nears - Sep 1

Wisconsin Bans Trashing of Electronics - Sep 1

Amazon Kindles Connect Rural Libraries to Digital World - Aug 31

Economy Forces County IT Departments to Embrace Practicality - Aug 31

Briefs: McKinney, Texas, Hires Former Colorado Springs IT Manager - Aug 31

[View All Government Technology News](#)

Industry Solutions for Government

Read real world deployments of technology in government from our sponsors.

Cyber Security Cases

Economic Development Cases

Enterprise Cases

[View All Industry Solutions](#)

Marketplace

SAS earns top ranking in predictive analytics and data mining. [Read report.](#)

[Read this four-part series on realizing a more accountable government.](#)

[See how Adobe opens up government](#)

[Road Map to the Virtual Data Center – Journey to the Private Cloud](#)

Related Products and Services

Ensure device & data security as well as reliable connectivity with Security & Management Solutions : Hewlett-Packard

We help state and local governments connect to citizens with our services, learn more here. : Pitney Bowes Business Insight

