SailPoint

SOLUTION BRIEF

The 3 Steps for Securing Sensitive Citizen Data

Gartner estimates 80% of all data in the world is stored in files, and oftentimes, these files are stored in insecure locations. Furthermore, many state and local governments and agencies have no visibility into where these files reside, what each file contains and who can access this data. This gap has the potential to improperly expose sensitive citizen data to individuals or groups with questionable or even malicious intent. If you don't know where sensitive data resides, you cannot protect it.

For this reason, the public sector needs identity governance capabilities that extend beyond databases and applications. They need visibility and control of data files that can be stored in less secure locations such as network file shares, SharePoint and cloud drives. How do you close this gap? Where do you start? With the state and local governments and public agencies typically understaffed and under-resourced, approaching this mammoth task can lead to a sense of futility that results in inaction. It doesn't have to be that way.

With 80% of all data located in digital files, public organizations must exercise precision in securing the most sensitive data.

Understanding the Data Lifecycle

Governments and public agencies regularly operate a variety of systems and applications. Often, sensitive information migrates from these secure databases and into less secure locations. For instance, a state education department administrator compiling a report on the student population may access sensitive data from the learning management system (LMS) and then place that data into a presentation. A county health department staff member doing research may export a set of data that includes personal identifiable information (PII) and protected health information (PHI) from a clinical system only to be saved into a spreadsheet. Typically, this data is then stored in network file shares, SharePoint and cloud drives. These locations are typically vulnerable to exposing sensitive citizen information to prying eyes.

How to Secure Files with Sensitive Data

Once you understand the challenges associated with governing data within the public sector, risk levels become apparent. Building a game plan for securing citizen information is critical. A law enforcement agency is subject to Criminal Justice Information Services (CJIS) audit. Health departments must abide by Health Insurance Portability and Accountability Act (HIPAA) regulations. Publication 1075 compliance applies to all tax and revenue departments. Failing to comply with such regulations can result in significant financial consequences and a tarnished reputation. So how does a public organization beholden to all these factors successfully drive toward compliance? The steps below outline how to inventory and classify data, create governance around access to the data, and assign ownership:

1

Step 1: Discover and Prioritize

The amount of sensitive data stored in files is growing at an exponential rate. Just locating data files, much less managing access to that information, can be overwhelming and lead to complacency with the status quo. To streamline efforts and minimize impact on IT resources, a targeted approach is far more reasonable and achievable. Rather than boiling the ocean, governments and public agencies should conduct comprehensive discovery to flag files that contain sensitive content. This enables them to prioritize efforts and exercise precision in securing the highest-risk files.

2

Step 2: Assess Users

Analyze who has access to and who is accessing sensitive data (employees, contractors, vendors, business partners, etc.). While these two groups may overlap, they are not necessarily the same. To control and govern access to sensitive data, it is critical to build out a model that correctly identifies users who have business justification to access specific types of sensitive data. Organizations need to automatically compare the actual state-of-access with the desired state and eliminate overentitled users on a regular basis. This can be formed through regular access review processes, or more automated reconciliation tasks. This assessment will help set the foundation of critical governing policies moving forward.

3

Step 3: Empower Data Stewards

Within any organization, who would have the best understanding of which users should have access to what and when? While IT departments often end up with the responsibility, they rarely know the data or the users. On the other hand, data stewards have contextual understanding of the data and users, and usually have the bandwidth to govern access. For these reasons, it is essential that governments and public agencies determine and designate appropriate data stewards who have knowledge of and familiarity with the data to properly administer it. These individuals are best positioned to govern approval processes (access certification and requests) and to review and address access violations.

As you set policies around access, it's important to ensure the processes for granting and validating access are conducive for the desired security results, while minimizing impediments to users' day-to-day operations.

The SailPoint Advantage

SailPoint helps governments and public agencies mitigate cybersecurity risks and maintain compliance with a comprehensive identity governance solution that applies to all data wherever the information resides. Our approach streamlines the process for finding sensitive content in files and documents located throughout the organization. SailPoint further enables IT administrators and data owners to prioritize and manage who has access to content that pose the greatest cybersecurity and compliance risks.

Furthermore, SailPoint is recognized by Gartner and Forrester as the leading authority in identity governance and administration. This is essential because knowing and governing identities is a central tenet to protecting sensitive information and ensuring reasonable freedom of access for those who legitimately require information as part of their daily workflow. SailPoint provides various benefits to public sector organizations:

Enhance visibility into PII, PCI, PHI and other sensitive data

- Locate and classify sensitive data based on content or who is accessing data
- Support more intelligent governance decisions with deeper insight about users and access that provide complete identity context
- Monitor on-premises and cloud data access in real-time

Drive compliance with corporate and regulatory requirements

- Help drive compliance with proven policies, rules and search expressions
- Streamline access reviews and certifications to quickly respond to audits and maintain compliance
- Maintain a real-time health status across all governed data sources and act on potential compliance risks

Establish governance control with business accountability

- Utilize targeted crowdsourcing to more accurately identify owners responsible for sensitive data
- Ensure only authorized users are provided access with streamlined access requests
- Detect and respond to policy violations in real-time with automated alerts

Remediate risk with actionable intelligence

- Enable IT, security and business users to identify and remediate risk with actionable dashboards
- Address entitlement creep and establish one permission path per user with access normalization and cleanup
- Avoid human errors while reducing IT workload with automated access fulfillment

If you are interested in learning how our solutions can help state and local governments and public agencies to locate, secure and manage sensitive data and files, **contact us to set up a demonstration.**

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.

SB1194-1801