5 Essential Data Compliance Best Practices for Government Agencies

The public sector deals with a treasure trove of sensitive data, from social security numbers to payment information. Hackers know this and have increasingly turned their focus to local and state government agencies. Consequently, these organizations must implement data compliance best practices to safeguard personally identifiable information (PII) and avoid stiff penalties.

For example, in 2016, dozens of Los Angeles County employees gave in to a phishing attack. As a result, hackers gained access to the personal data of nearly 800,000 people. Attackers can then sell personal information or use stolen credentials to access government systems or disrupt critical services.

In response to attacks like this and a growing demand for data privacy, all states have enacted security measures to protect sensitive data. And as of 2020, at least 32 states have passed data privacy legislation that applies to government agencies. The following best practices will help these agencies meet common data privacy requirements.

1. Conduct Security Assessments

Several states require that agencies implement a system of regular security assessments. Even when assessments are not specifically required, the audits deliver significant benefits as part of an overall security strategy.

For instance, security assessments serve to highlight vulnerabilities and areas for improvement. Forward-thinking agencies also use them to raise awareness, measure security training programs and develop action plans for strengthening cybersecurity. In addition to annual audits, continuous, automated monitoring provides ongoing protection.

2. Address the Human Factor with Security Training

Employees present the largest risk to data compliance. In the course of their day-to-day duties, even low-level employees have access to significant amounts of sensitive data. An employee who uses a weak password or clicks on a malicious link in a phishing email can inadvertently expose thousands of records.

To guard against preventable leaks, organizations should conduct regular, targeted security awareness training. Employees need to understand agency security policies, including best practices for passwords and file sharing. They should also learn to thwart phishing scams and recognize anomalies that may indicate a security incident.

3. Monitor Third Parties

In February 2021, a billing services company suffered a ransomware attack. Because the company contracted with the California Department of Motor Vehicles, the attack also exposed driver and vehicle records stretching back over 20 months. In many cases, government agencies remain liable for such data breaches, even when they occur through a third party.

To demonstrate data compliance, government agencies must carefully address their vendor agreements. Begin by ensuring that contracts with third parties include the stipulation that vendors maintain reasonable security practices around sensitive data. Additionally, make sure you know and monitor all third-party access points to agency networks and data.

4. Create an Incident Response Plan

In today's cyber climate, organizations should expect to experience a data security incident, regardless of their cybersecurity strategies. Knowing this, many data privacy laws require agencies to implement cybersecurity incident response plans. With a plan in place, the agency can act quickly when an incident occurs, minimizing damage to sensitive data and systems.

Incident response plans should include contact information for key personnel and a prioritized inventory of IT assets. The plan will outline immediate response steps, as well as recovery plans. And a detailed communication plan should cover communication with employees, as well as with media and customers.

5. Establish Security Policies and Automate Where Possible

Each agency should develop information security policies, covering practices such as email encryption and the storage and disposal of sensitive data. ePolicies not only serve to protect PII and ensure regulatory compliance, but they can also help to reduce storage costs. In many instances, these policies can be automated, thus minimizing risk from human error.

Implement Data Compliance Best Practices with Expert Help

The data compliance experts at Messaging Architects make it their business to know the data privacy landscape. We offer data compliance and security assessments, ePolicy consulting and a wide range of compliance and cybersecurity services. Act now to secure sensitive data and maintain regulatory compliance.