FROM DEVICE TO DATA:

Creating an Efficient Workflow with Security in Mind in State and Local Government

State and local government agencies store an abundance of constituent data, making them a prime target of cyber attacks.

THE AVERAGE COST OF A US DATA BREACH IS
$8.19
IN 2019.*

THE AVERAGE COST PER RECORD IS
$242.*

THE AVERAGE NUMBER OF RECORDS IN A SINGLE DATA BREACH IS
32,636 RECORDS.*

This infographic highlights some common areas of potential vulnerabilities in a government employee's workflow. It also shows the access controls that can be used to help secure documents, increase efficiencies, and support compliance strategies — allowing an agency to focus on its core mission of improving constituent services.

PRODUCED BY
CENTER FOR DIGITAL EDUCATION

SPONSORED BY
Canon
CANON SOLUTIONS AMERICA

⚠ Layered Security ⚠

Layered security comprised of device security, print security, information security, and cyber security, resulting in a comprehensive approach to protecting your agency.

⚠ Automatic Alerts ⚠

An administrator can be alerted should someone attempt to print, scan, or copy sensitive documents that contain keywords (confidential, sensitive, etc.).

⚠ Defense at Device ⚠

Before accessing a device to print, scan, or copy, a government employee can use an authenticated ID card to help gain the appropriate level of access.

⚠ PII Protection ⚠

A government employee can print information or records from a mobile device, which are then held on a server with security features until he or she enters a password at a printer to retrieve them.

⚠ Compliance ⚠

A layered approach to protecting your organization can establish an effective security posture and thus facilitate compliance with regulatory guidelines.

Collaboration without ⚠ Borders ⚠

When collaborating with staff and other departments, enterprise digital rights management (EDRM) tools enable administrators to control file level access to help ensure that information is not compromised.

2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.

Canon U.S.A., Inc. and Canon Solutions America, Inc. do not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GDPR, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.
Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance.
Some security features may impact functionality/performance; you may want to test these settings in your environment. Neither Canon Inc., Canon U.S.A., Inc. or Canon Solutions America, Inc. represents or warrant any third-party product or feature referenced hereunder. As of November 2019.