A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

From Threat to Trust:
Building Security into Public Workflows

SPONSORED BY hp / intel

Public sector organizations must defend an increasingly complex attack surface. Remote work, third-party access and the adoption of AI tools without clear governance have expanded the number of potential entry points for attackers.

Unfortunately, many modern attacks are subtle and credential-driven, allowing threat actors to infiltrate systems through stolen identities and social engineering techniques before moving through networks undetected by traditional defenses.

To protect against these evolving threats, agencies can no longer rely solely on add-on security controls. Instead, security must be embedded directly into the tools and workflows employees use every day to safeguard a growing number of endpoints.

Making Security Intuitive

"Security works best when it's designed into everyday workflows from the start and aligned to how people actually do their jobs," says Michael Dent, a senior fellow at the Center for Digital Government. "Security only feels restrictive when it's added after decisions are already made."

By making security a foundation of employees' typical processes, agencies can make protection a normal part of workplace operations rather than an additional step.

"Security without usability won't be adopted, and performance without security won't be deployed," says Leonard Isler, global SME for data science, AI and machine learning at HP. "You have to treat them as co-requirements, not as separate things."

No matter the capabilities of security tools, the safe use of equipment comes down to team members. It's critical to communicate why solutions are in place and how they benefit the organization.

Leadership must be ready to:

- Discuss any changes with team members and take their feedback seriously
- Integrate new policies into onboarding and training
- Create clear and widely applied policies that serve as the foundation of security
- Set consistent expectations for how devices and solutions will be used across teams and departments
- Define roles and responsibilities and address how they may change

"The difference between success and failure is when leadership treats security processes as core principles or optional guidance," Dent says.

To cover today's growing attack surfaces, agencies should adopt security controls that cover the full breadth of systems and workflows across diverse devices, applications and networks. Specifically, agencies need device-level protections, which are built into the equipment (phone, tablet, laptop, etc.) itself, to secure any data stored on a device.

These tools automatically prioritize passwords and authentication, encrypt stored data, check the safety of software before running it, and update security patches.

Device-level protections empower agencies to strengthen overall security posture and resilience — to shift from reacting to threats after they occur to proactively maintaining trust and reducing risk across all endpoints.

This strategy makes sure any processes on a device are protected. Add-on solutions that only monitor specific apps leave too much risk.

Maintain awareness by providing training and showing examples of suspicious activity such as phishing attempts.

Best Practices

1. **Begin with procurement.** Start assessing devices at the procurement stage. If tools can't align to your security processes, don't buy them.

2. **Establish a Zero-Trust architecture.** With this strategy, no device or user is automatically trusted. Instead, organizations must deploy multifactor authentication and least-privilege access.

3. **Share and collaborate with others.** If you communicate regularly with peers, add built-in security to your list of discussion points. If you don't check in with other groups yet, use this as an excuse to get started.

4. **Offer regular training.** Human error still plays a massive role in cybersecurity. Maintain awareness by providing training and showing examples of suspicious activity such as phishing attempts.

5. **Strive for continuous improvement.** Risks are quickly evolving in number and sophistication. Leadership must stay up to date on advancements to protect their staff, equipment and the people they serve.

6. **Don't ease up on data protection.** Security is not something that can be set once and forgotten about. Agencies that manage sensitive data must make sure it's always protected. That means encrypting data in transit and at rest. Data classification and labels can help efficiently find data when it's needed while mitigating risks.

Building Trust Through Security

As public sector organizations navigate more complex threats, the conversation should extend beyond individual security tools or isolated controls. The greater challenge is determining how security, workforce practices and technology investments can work together to support mission outcomes while maintaining public trust.

Leaders should evaluate how security is embedded across the employee experience — from procurement and device management to collaboration, data governance and ongoing workforce readiness.

Organizations that take a holistic approach will be better positioned to strengthen resilience, improve operational continuity and adapt to an evolving threat landscape.

Building security into everyday workflows is not simply a technology initiative. It's an opportunity to create a foundation that enables innovation, supports organizational agility and helps agencies confidently serve their communities in a rapidly changing environment.

This piece was written and produced by the Government Technology Content Studio, with information and input from HP Inc. and Intel Corporation.

Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Sponsored by HP Inc. and Intel Corporation

HP Inc. is a technology company that believes one thoughtful idea has the power to change the world. Its product and service portfolio of personal systems, printers, and 3D printing solutions helps bring these ideas to life.

www.hp.com/HPSolutions-StateandLocalGov

Intel Corporation is a company with the purpose to create world-changing technology that improves the life of every person on the planet.

www.intel.com

©2026 e.Republic LLC. All rights reserved.