

How to Build a People-First Culture



Culture is a small word that carries a lot of weight.

It's the intertwined dynamics of unspoken rules, policies, employee ethos and the mindsets and risk tolerance of leadership. Culture determines if the initiatives, new technologies and practices introduced within an agency will take root and thrive or quickly flounder.

In this resource, we touch on several aspects across the workplace, including collaborative workflows, data literacy and secure hybrid work, all of which require employee buy-in and a people-centric mindset to succeed. You'll also hear from human resource professionals who speak to the needs and concerns of employees who are navigating the workplace amid constant change.

Our subject-matter experts first shared their insights during GovLoop's virtual summit, "[How to Build a People-First Culture.](#)"



Do Your Legacy Workflows Need a Refresh?



Michael B. Jackson

DocuSign



G. Nagesh Rao

Commerce Department

The public sector runs on workflows, so what happens when these processes cannot move freely?

The answer: Little that can help citizens quickly or efficiently. For too long, agencies have used paper-based processes to deliver products and services. As the COVID-19 pandemic has made clear, these legacy workflows need a refresh.

Enter digital workflows. Digitizing processes like document signing can make them more resilient to crises like COVID-19. Even better, digital workflows can overcome many of the collaboration issues their paper-based counterparts have.

"It shined a spotlight that said, 'We've got to do better,'" Michael B. Jackson said of the COVID-19 pandemic. Jackson is AVP, Global Head of Industries, Public Sector, Healthcare, Life Sciences, Financial Services at DocuSign, a cloud-based electronic agreements management provider.

Jackson and Chief Information Officer (CIO) G. Nagesh Rao of the Commerce Department's (USDOC) Bureau of Industry and Security (BIS) shared three reasons why agencies should digitize their workflows for stronger collaboration.

Reaching Resilience

Resilience is the ability to respond to, recover from and continuously operate during disturbances. It's a crucial quality for governments during emergencies.

But paper-based workflows are often at odds with the benefits of resilience. Paper's physical limitations make it more vulnerable to external and internal threats, and paper-based workflows are less accountable and transparent than digital ones.

"Paper is physically susceptible to things like fires," Jackson said. "And, until a form or record is digitized, it is difficult to share, collaborate on, archive and analyze."

Digitization can not only remove paper's material shortcomings from the equation – it can make agencies' content easier to find and share with the right teams.

Craft Collaboration

Internally, digitized workflows enable government employees to collaborate in real time on important work no matter the distance. Externally, constituents can more readily access government services electronically and, in many cases, experience faster approval processes for things like benefits when key documents are efficiently routed internally.

"You can make a decision much faster as people can all access it at the same time virtually," Jackson said.

Take marriage licenses. Rather than physically passing such important documents through the chain of people who need to approve them, digitization can make the entire workflow quick, electronic and seamless.

Augment Intelligence

Emerging technologies such as artificial intelligence (AI) and automation are all the rage, and for good reason; AI mimics human cognitive abilities like reasoning, while automation performs simple, manual tasks without people being involved.

Digitization makes applying automation and AI to workflows simpler. For instance, digital records management platforms make it easier to locate documents using keyword searches.

"You're trying to augment the decision-making process," Nagesh said of tools like AI. **"You can really use them to transform digitally. But at the end of the day, the human still needs to be there."**

At heart, government is about people working together. By digitizing workflows, agencies can streamline and enhance interactions among employees and with the constituents they serve.

Practical Ways to Cultivate a Data Literate Culture



Scott Beliveau
U.S. Patent and Trademark Office



Chezhain Sivagnanam
U.S. National Science Foundation



Andy Maclsaac
Alteryx

Here's the deal: As long as data is left solely in the hands of data scientists, its impact will be limited.

Yes, data scientists play a vital role in driving key data initiatives and supporting major programs. But for data to become an integral part of how agencies make everyday decisions about policies, programs and services, data needs to be embraced by their everyday decision-makers.

"It's more about people than technology," said Scott Beliveau, Branch Chief of Advanced Analytics at the U.S. Patent and Trademark Office. **"It's about engaging folks, getting them to ask questions, getting them excited about answering those kinds of questions, and empowering them with the tools, technology and knowledge to become successful."**

In short, it's about cultivating a culture of analytics for everyone. Here are some ways to make that happen.

Develop Data Smarts

Developing data smarts once required significant technical expertise, but that's no longer the case. The emergence of low-code/no-code solutions and self-service platforms make it possible for non-experts to begin digging into data without extensive training.

Training is still important, not in the technology but in data itself, said Chezhain Sivagnanam, Chief Enterprise Architect at the U.S. National Science Foundation.

"It's about providing a clear documentation of how to use the data, and making sure they are educated on...data policies, data lineage and all that goes with the data," he said.

Get Specific About the Benefits

Organizations often launch data training initiatives with much fanfare, but with little discussion about the practical benefits of analytics, said Beliveau. The result? People lose interest.

Beliveau points to the physicist [Richard Feynman](#), who in 1959 got his CalTech students interested in the nascent field of nanotechnology by posing an intriguing challenge: "Why can't we write the entire 24 volumes of the Encyclopedia Britannica on the head of a pin?"

"You need to tie [data] to a specific, immediate goal that benefits people," he said. "Articulate that, 'Hey you're going to save time, or you're going to avoid work.' Then it becomes more of an organic thing."

Treat Data as a Team Sport

Data experts still have a role to play, of course, but as part of a larger team.

"You have to look at data and analytics as a team sport," said Andy Maclsaac, Solutions Marketing Director for Public Sector at Alteryx. "You've got your data folks, your business users, your domain experts – they all need to come together and collaborate."

In one case, Alteryx worked with a government agency in Great Britain that successfully integrated their data experts with the rest of the organization. As a result, "they've unleashed this curiosity within the business leadership, who are saying, 'I want more of this insight. How do we work together to get that?'"

Automation is vital to feeding that hunger. "If you're spending all your time cutting and pasting from one spreadsheet to another, you're going to burn out your team, leaving them less bandwidth to do higher level, more impactful analytics," he said.

How to Wrap Your Head Around Zero Trust Security



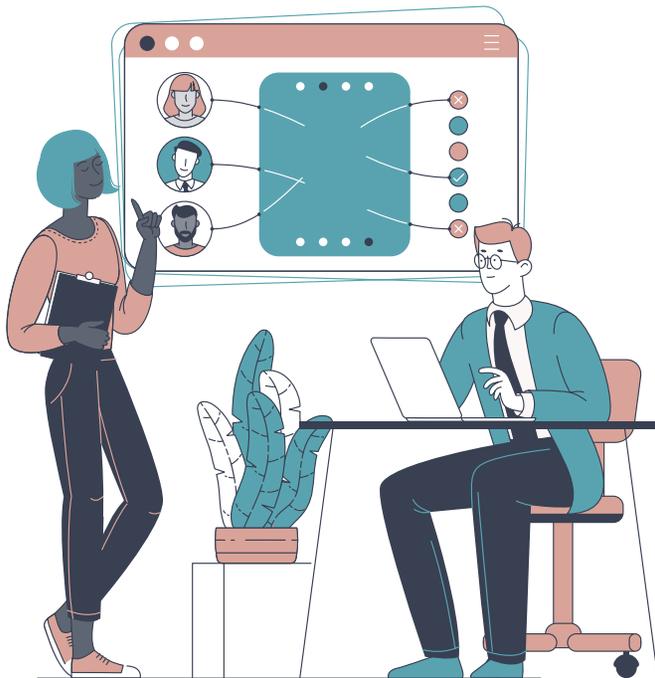
Mike Epley
Red Hat

Zero-trust security would be a lot easier to understand if there were a zero-trust product that agencies could buy. But it's not that easy.

In practice, zero trust can involve a number of solutions, such as network access controls, application-level security and identity and access management. But zero trust is more about principles than technology.

"The key here is altering our traditional security thinking, and thinking more from an enterprise and holistic perspective," said Mike Epley, the Chief Architect of Public Sector at Red Hat

Here are three key concepts that can help you understand that holistic perspective.



Denial Boundaries

"Deperimeterization" is a phrase commonly used to explain zero trust, but what exactly does that mean?

Think about virtual private network (VPN) technology, which has been an essential solution for many agencies during the pandemic. A VPN enables someone working remotely to tunnel into their agency's network and appear as if they were in the office. In this model, access controls are tied to the underlying architecture and physical locations of the network, which divides the world into insiders and outsiders.

Zero trust, on the other hand, establishes a denial boundary unrelated to the location of the user trying to access a network resource, or to the location of the network resource, Epley said. That user is denied access until authorized by the network.

"Zero trust assumes that we have the default hardening and protections for our systems and can enforce that denial boundary," he said.

Explicit Access

If security controls are not tied to location, what is the basis for approving or denying access? It's a matter of necessity. Zero trust requires organizations to make conscious decisions about who gets access to what resources – that is, to establish an explicit business need for someone to access a given resource.

"The [Defense Department] has long had this concept of 'need to know,' and this is the foundation of many of their access controls already," Epley said.

For many civilian agencies, need often is left implicit. Access is often driven by the original business requirements of a system, which defined the intended users, but "it's not explicitly defined, and the business driver essentially allows access regardless," Epley said.

Contextual security

Zero trust also requires a more contextual approach to access controls, both in terms of the privileges given to users and the risks involved.

"Even if we can assert a business need, we continuously revisit and reevaluate that access, and those access controls, in light of any changes to the system or the users that are interacting with that system, or other aspects," Epley said. "Then we make access decisions dynamic based on that context."

The challenge is that agencies don't have the luxury of building a zero trust architecture from scratch but instead must work with their existing security solutions and tactics.

"We now have to evolve those systems accordingly and, of course, keep them operational, keep them usable," Epley said.

3 Ways to Support Secure Hybrid Work



Jose Arvelo
Citrix Systems, Inc.



Mika J. Cross
Strategic Advisor

Hybrid workplaces have swiftly moved from being a perk to an expectation. And agencies leading this massive shift are those that have adapted their thinking around cybersecurity.

“Agencies who are getting this right [are] evolving their strategy around creating this workspace culture,” said Mika J. Cross, a Strategic Advisor for the federal government. **“It’s really a placeless mindset but where everybody feels like they’re a part of a secure culture.”**

From a technology and accessibility standpoint, there are two key issues driving this change, said Jose Arvelo, Senior Director of Federal Engineering at Citrix Systems, Inc.

- ↳ Where IT services, applications and data are located is shifting more and more away from the data center and into the cloud.
- ↳ Security needs to be closer to the end user. People are working from home networks that are connecting to government data centers via virtual private networks or VPN.

“There’s a new set of risks that agencies have had to consider as a result from both of those different shifts,” Arvelo said. Here are some considerations to keep in mind.

Rethink the VPN strategy

If Arvelo had his way, organizations would ditch VPN altogether. The reason being is many employees are relying on home networks that agencies don’t control. They also don’t control other devices that connect to that network.

“Let’s get rid of the virtual private network and replace it with secure digital workspaces,” he said. Rather than employees being tied to one device, network or geography, they have the flexibility to securely access their workspaces from anywhere while remaining productive.

Balance security and user flexibility

Unlike a traditional VPN, Citrix Secure Workspace Access, for example, provides a zero trust approach to securely access enterprise web, cloud and virtual applications. Security levels can be adjusted based on the user, where they are located and the security posture of the device, Arvelo said. “Now you have a more flexible and targeted way of approaching cybersecurity.”

But no cybersecurity solution or strategy is going to be successful unless it is acceptable to the end user, Arvelo said. There must be a balance between security and flexibility.

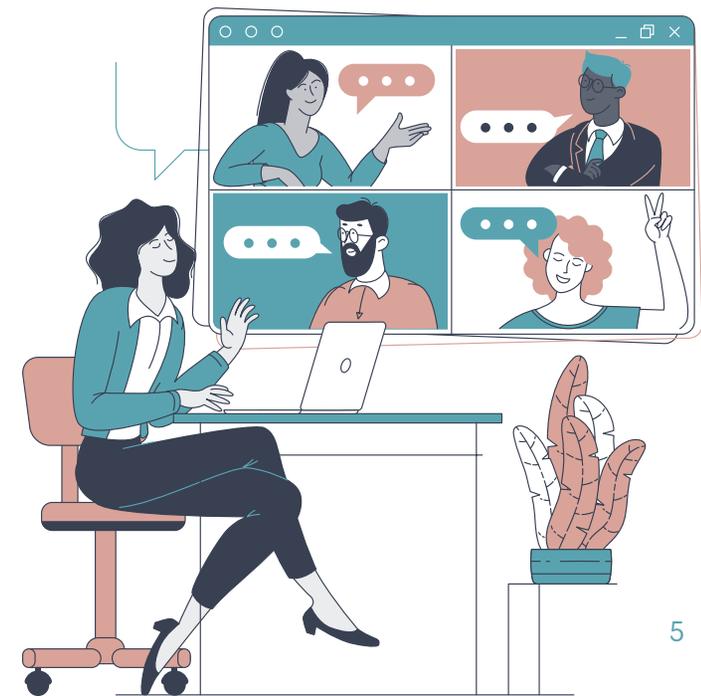
“I know it’s very difficult, and everyone likes to talk about it like it’s an easy thing,” he said. “It’s really not.”

Make security part of workplace culture

“I just challenge everyone to think about ways that you can normalize conversations around security and everyday work,” Cross said.

Maybe that entails having an informal recognition program for spotlighting someone who flags a security issue or raises a question or issue – no matter how small. There are opportunities for team-based, Jeopardy-style training to gamify learning and create a culture where people feel safe asking questions or saying they made a mistake.

“It’s building camaraderie and enhancing the work environment,” Cross said.



SBA's Journey to Simplify Cybersecurity



Sanjay Gupta
Small Business Administration



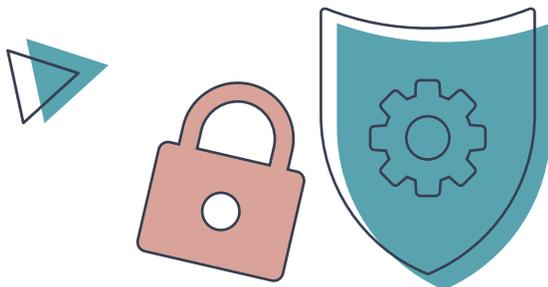
Tom Roeh
ExtraHop

Chief Technology Officer Sanjay Gupta has a unique philosophy that guides his cybersecurity practices at the U.S. Small Business Administration (SBA).

"I believe in simplicity and, certainly, that is one of the hallmarks that I believe in cyber: It's easier to make things complex, but it's more difficult to make it simple," Gupta said.

A few years ago, he had the opportunity to define a vision for cyber and protecting all of SBA's information technology assets. The agency needed a singular and uniformed way to manage, monitor, track, and secure all IT assets. That included assets in the cloud, on premises, collocated in data centers, mobile assets and everything in between.

This massive undertaking would prove to be a defining and very forward-thinking move as SBA was thrust into a spotlight role when the COVID-19 pandemic hit.



Challenge

The agency has been at the forefront of one of the nation's largest economic recovery initiatives, having processed more than \$1 trillion in loans and capital for small businesses. For comparison, pre-COVID-19, the agency used to process about \$30-\$35 billion in capital annually.

"So, as you would imagine, we have become a target more so than ... we had anticipated for the bad actors," Gupta said.

Solution

But employees didn't shrink back from their newfound responsibilities, he said. They collaborated.

"There's no single organization in my view that has the wherewithal to be able to manage, monitor, secure, everything that they're faced with," Gupta said. "So what that means is, you have to collaborate, you have to partner with industry partners, with other federal agencies like CISA [Cybersecurity and Infrastructure Security Agency] and others, and be able to join forces and be able to put up a unified front in dealing with these things."

This collaborative approach is critical, especially because many organizations often lack staffing and adequate training, said Tom Roeh, Director of Systems Engineering at ExtraHop, a cloud-

native cybersecurity solutions provider. He stressed the importance of prioritizing these shortfalls through adequate budgeting and complementing staff expertise with the right tools and technologies.

"Just buying a product doesn't necessarily [mean] it's going to solve all your problems," Roeh said. "You've got to build the right processes and, ultimately, the right culture around those tools."

As you consider simplifying your security environment, Gupta and Roeh shared these tips to consider:

- ↳ **Review the IT tools you've purchased** but have allowed to sit on the shelf and collect dust. By simplifying your inventory, you may find additional resources that you can redirect toward hiring or training.
- ↳ **Determine who needs access to what.** SBA uses a set of dynamic policies and configurations called conditional access that requires certain conditions (IP address, risk behavior, etc.) to determine what level of access a user should have.
- ↳ **Consider the cloud.** Many agencies that have embraced cloud-based security have been better positioned to adapt to changing workforce and constituent needs during the pandemic.

Putting People First in the Future Government Workforce



Jeff Birch
Federal Acquisition Institute



Lisa Munzenmaier
SAP NS2

The future of government workforces is here. Going forward, most agencies will need hybrid workforces mixing on-site employees and remote workers.

How can these agencies put their people first when most individuals will not be working face to face? Federal, state or local, agencies will need to engage, excite and fulfill their hybrid workforces.

According to Jeff Birch, Director of the Federal Acquisition Institute (FAI) and Lisa Munzenmaier, Director of SuccessFactors Solution Management at SAP NS2, a software provider, agencies have the tools to create tomorrow's workforce today. To build future-ready operations, agencies can combine professional development with collaborative technology like cloud computing here and now.

"Employees want to feel like they're adding value, using their skills and providing a benefit," Munzenmaier said. "As organizations, we need to make sure we're providing that environment."

Birch and Munzenmaier detailed three ways that agencies can fuel constant development and growth wherever their workers are.

Cultivate Continuous Learning

People love controlling their own destinies, and government employees are no exception. Fortunately, technology has revolutionized agencies' training by enabling continuous learning. Leveraging continuous learning, public-sector workers can chart the education paths that are best for them.

"This allows people to take their courses when they need them when it fits their working schedules," Munzenmaier said. "It also gives people the opportunity to see that there are other courses out there that maybe they weren't aware of."

Take cybersecurity training. The cloud can store self-guided and instructor-led videos that teach workers about this crucial topic in the way that they prefer.

Facilitate Flexibility

Different employees have different needs, so agencies must carefully consider how to meet expectations while functioning effectively. To maximize mission wins, agencies should pair technology with the right user policies that benefit employees.

Laptop cameras are one example. Agencies with low employee engagement can encourage remote workers to use these devices during meetings; agencies with virtual meeting fatigue, meanwhile, can let employees turn their cameras off.

"What we are doing is ensuring we stay connected with our workforce," Birch said. "It is trying to think about work differently than how we have in the past."

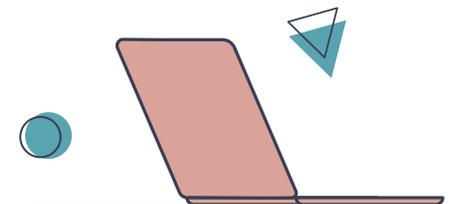
Agencies hungry for more flexibility should consider cloud computing. The cloud delivers computing resources like processing power on-demand, letting agencies adjust services like videoconferencing as circumstances change.

Balance Work and Life Better

Remote work has erased the barrier between work and home; it has also left many employees feeling like they cannot stop working.

To avoid hybrid workforce exhaustion, Birch recommended that agencies encourage rest regardless of where their employees work. "We need to try and set a timeframe where we have a disconnect," he said.

No matter the technology involved, Munzenmaier added, people must be at the center of every program and initiative. Organizations thrive when they elevate the needs of people and allow those needs to guide decision-making.



Career Corner: GSA's HR Exec Answers Your Burning Questions

Do you know what will differentiate you from being just an employee to a good employee? The answer is both simple and complex.



Traci DiMartini
GSA

“What makes a good government employee isn’t that different from what makes a good employee, period. **But we do have a necessity to have a passion for public service,**” said Traci DiMartini, Chief Human Capital Officer for the General Services Administration (GSA).

Public service is a calling, DiMartini said. You may not receive riches and recognition – but you do the esteemed work of providing essential services to the public, whether you’re a frontline agent at the Social Security Administration or an IT jack-of-all-trades in a local government.

In addition to having a passion for public service, being a good government employee comes down to general practices, such as:

- **Having humility.** “Everyone starts at the bottom,” DiMartini said. In addition to patience, humility is essential. Learn how to take directions and work (and play) well with others, she said.
- **Having a sense of humor,** especially when it comes to mistakes. For many employees, mistakes are ultimately recoverable and correctable. Practice learning how to build alliances to figure out a way forward.

The following are other career questions DiMartini answered. Check to see if you have asked any of the same.

How can employees grow professionally when their bosses are closed off to trying new things?

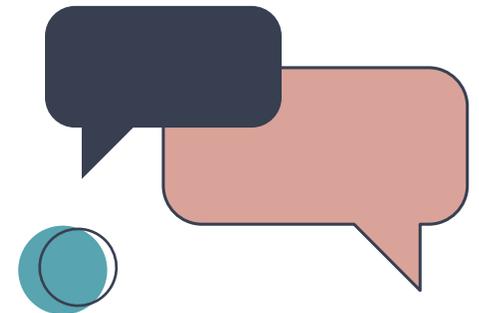
“Never believe that anyone can stop your growth,” DiMartini said. Even if you can’t attend a training program, or your idea isn’t implemented, the process of trying is still an opportunity for growth and development.

But, additionally, ask your boss why – and approach the question in a positive, open-minded way. Your boss probably has a good reason. Bureaucracy doesn’t exist for the purpose of slowing things down, but to prevent bad decision-making and ensuring different angles are considered. Your boss may have experienced or seen something you may not have seen or experienced. It doesn’t hurt to ask, but approach the conversation assuming the best.

How can we help coach government employees who are feeling burnt out?

Help them prioritize properly. Supervisors should be in the weeds with their team – not doing their work for them, but understanding what their loads are like and prioritizing realistically.

“We also have to acknowledge things are hard,” DiMartini said. We all recognize there’s really no good time to be out of the office – but taking time off remains important to avoid burnout.



How can we work cross-generationally? And motivate the next generation of the government workforce?

"Learning can happen both ways," DiMartini said. For example, older generations can learn how to capitalize on technology from younger generations, and younger folks can learn from the experience and skills of older folks. DiMartini believes government can be more successful if everyone respects and acknowledges that "each generation brings something to the table that can be useful for the generation above and below."

How do you keep employees engaged in the remote and now hybrid work environment?

Until DiMartini can return to headquarters, hosting structured and unstructured Zoom meetings with colleagues has worked – as well as respecting that people have lives outside of their work. "They spent all of August learning about my empty nest syndrome," she said. Once more and more people return to the office, teams will have to tackle and right-size how important face time actually is. Just because you see someone in the office more does not necessarily mean they're better employees, she pointed out.

How do you help develop people's skills post-pandemic?

Focus on transferable skills. "You can be the smartest procurement officer in the world, but if you can't open your mind to doing things differently or learning new skills, you're going to hit a wall." Sometimes referred to as "soft" skills, DiMartini prefers calling them "strength" skills.

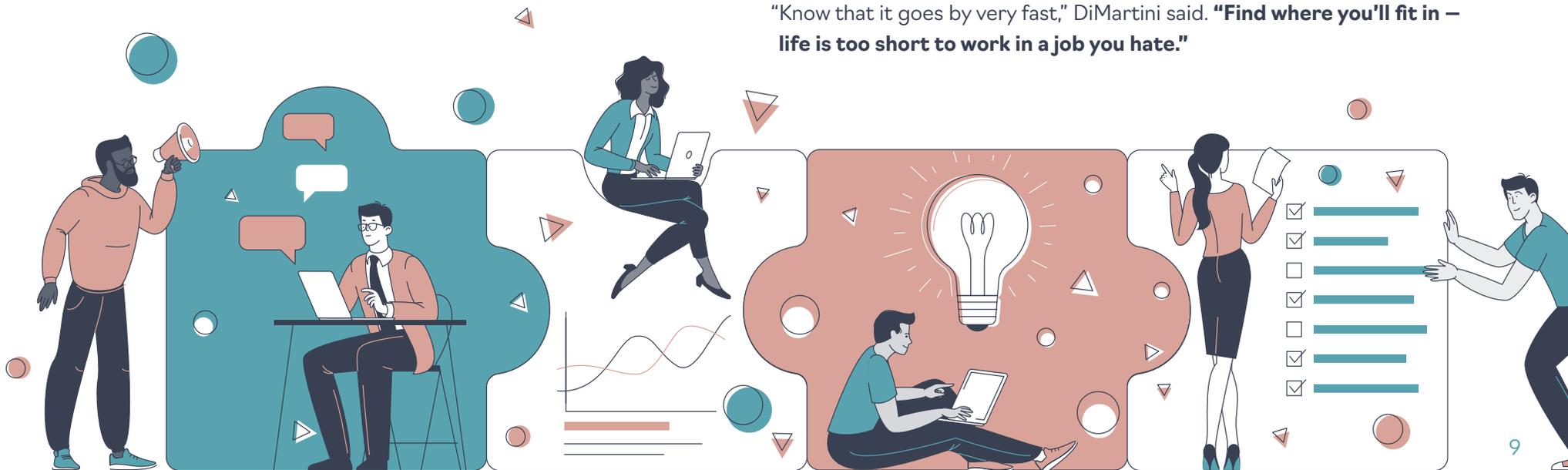
Don't underestimate the value of failure as well. "Sometimes, failure will teach you things success never will," DiMartini said. Learning how to handle failure and take risks in a calculated way will be valuable wherever you go.

How do you differentiate between having a bad day and being in a bad workplace?

"Sometimes you just have to sit with it and wonder what else is going on," DiMartini said. She listed some questions to ask yourself: Am I reacting because there are external, non-work-related factors that are making things amplified? Is it one specific issue, or a calculated series of issues? Can I build resilience and tough it out for a year, as long as I'm not being harmed?

What is one takeaway you'd like to leave people with in regard to their career?

"Know that it goes by very fast," DiMartini said. **"Find where you'll fit in – life is too short to work in a job you hate."**





Lessons Learned From Memphis: Training and Motivating Employees in a Pandemic



Alex Smith
City of Memphis

When COVID-19 hit Memphis in March 2020, the city workforce and leaders needed to grow in ways they didn't expect before.

"Who knew I would have gone from chief human resources (HR) officer to chief safety officer?" said Alex Smith, Memphis' Chief HR Officer. She said her master's program in HR management did not equip her with infectious disease expertise. But learning how to overcome the challenge became a critical part of her job, with the opportunity to both grow professionally and serve residents.

Many employees stepped up to the plate to grow and take stretch assignments where needs were urgent. For instance:

- ↳ Fifty HR employees learned how to be internal contact tracers after being reassigned to the health department.
- ↳ Others ran vaccination sites.
- ↳ And one leader took over the whole internal contact tracing program, learning how to do it from scratch.

"That was a huge uplift for our community here. We've seen employees willing to take on new roles to support the operations," Smith said.

Here are five key elements the city emphasized to motivate employees and encourage them to take new opportunities.

- 1. Transparent communication.** "People who work in our organization are mission-driven and purpose-driven individuals," Smith said. So being clear about the needs of the city in a crisis and how employees could help support them made a persuasive difference.
- 2. Easy access to opportunities.** Employees should be able to take stretch assignments and new opportunities without getting bogged down by processes or culture.
- 3. Incentives,** such as out-of-class pay and bonuses, to help recognize the extra duties they take on.
- 4. Leaders.** They play an important role in encouraging employees to take advantage of growth opportunities by championing the value and benefits of gaining new skills.
- 5. Highlight success stories.** People tend to gravitate to an opportunity when they see others doing it. Highlighting individuals who have successfully completed training and made a difference in the organization can be motivating.

Conclusion

Whether the challenge in front of you is understanding how to use data in new ways, how to give employees secure access to internal resources or remaining nimble during the pandemic, each of these issues share a common thread: people.

A people-first mindset forces you to solve tough problems with your colleagues and constituents in mind. This mindset prompts you to consider how they will be impacted, what assistance they might need and whether a new path forward is needed.

Use the takeaways in this resource to tread new ground in your own career while uplifting and empowering those who work alongside you.

Thank you to our partners for their support of this valuable resource for public sector professionals.

alteryx

carahsoft.

citrix™

DocuSign®

ExtraHop™

Red Hat

SAP NS2
NATIONAL SECURITY SERVICES

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.



www.govloop.com
[@GovLoop](https://twitter.com/GovLoop)

