'disco' Meraki



URBAN TECHNOLOGY CHECKLIST

Building a More Connected Community

Based on a recent <u>GovTech handbook</u>, this checklist provides the steps governments can take to better connect their communities.

Building better communities through a foundation of connection



Support connected communities with IoT One-third of CDG survey respondents reported experiencing network constraints that hinder use of IoT devices.



Prepare for the future of work

Government leaders must build on early efforts in more sustainable ways to better serve constituents.



Bridge the digital divide

It's imperative that governments focus on the big picture—universal access, affordability, and adoption.

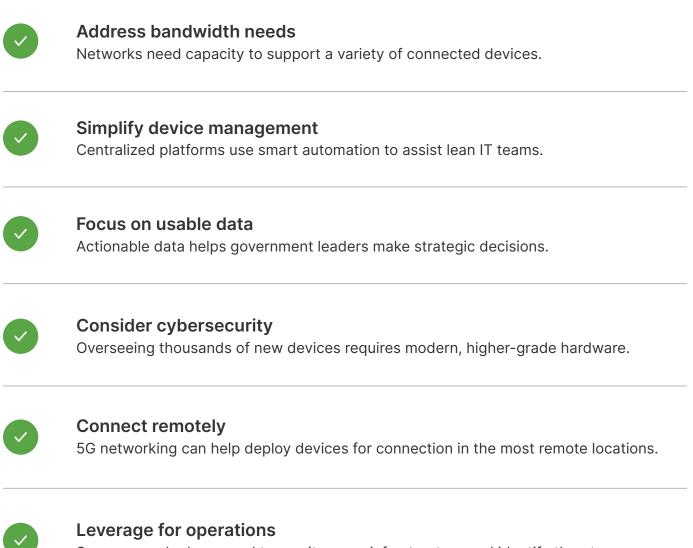


Securing IT all with ease

Securing connected community initiatives is an extension of the ongoing security focus for government IT.

Support connected communities with IoT

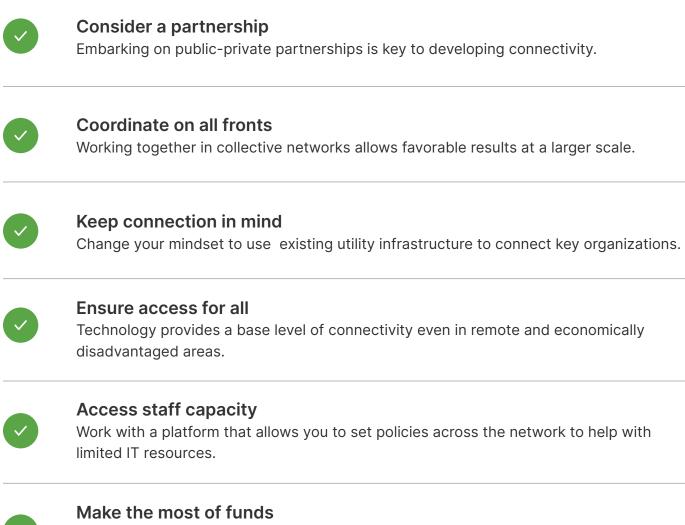
Developing strategies for deploying IT and technology devices is imperative for building connected communities.



Sensors can be leveraged to monitor your infrastructure and identify threats.

Bridge the digital divide

While broadband availability is the most visible constraint to universal access, affordability and adoption are also critical barriers.

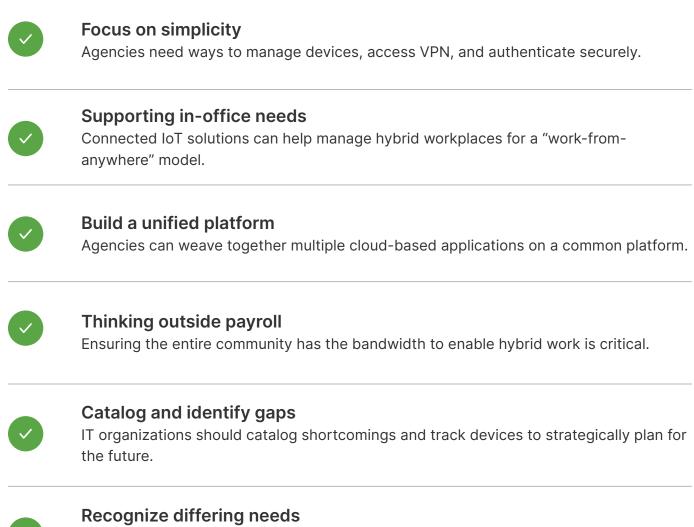


Governments need to navigate the requirements for federal grants to support technology purchases.



Prepare for the future of work

Keep sustainability at the forefront of planning to best preserve initiatives, especially while setting the foundation for a better future.



It's important to recognize that different agencies and functions require different tools to work effectively.



Secure IT for all with ease

Keeping sustainability at the forefront of planning is important to best preserve initiatives.



Set an always-on approach

Look to your utilities for a conceptual, consistent framework to help with risk mitigation.



Gather internal stakeholders

Security, connectivity, cloud, and operations all have critical roles to play in comprehensive security.



Identify critical needs

It is important for leadership to define a focus area as you begin your IoT security journey.



Ensure privacy standards

Secure data and sensitive information in ways consistent with federal guidelines.



Focus on training

Continue to establish training plans and periodically test employee knowledge.



Educate the community

Educate residents about cyber hygiene and help protect personal devices.

Ready to learn more? Download our GovTech Handbook.