ABOUT THE IOT GUIDELINES

These guidelines provide a framework to help government and our partners use connected devices and IoT technologies in a coordinated, consistent and responsible manner. They are intended to supplement – not replace – existing laws, rules, and regulations that apply to these systems. Special circumstances and concerns may also exist for IoT systems and/or data related to public safety, security and law enforcement.

Goals

The IoT Guidelines were created with four primary goals:

[1]

Provide a common framework to help government agencies develop and expand policies and procedures related to IoT.

[2]

Maximize transparency and openness regarding the design, installation and operation of IoT systems and how public privacy and safety will be protected.

[3]

Provide clarity on the minimum requirements and expectations for installing and operating IoT systems using public space or assets.

[4]

Advance the public dialogue about how government, the private sector and academic partners can maximize the public benefit derived from IoT solutions.

Background

By 2020, it is estimated that the number of connected devices (commonly referred to as the Internet of Things or IoT) will exceed 50 billion.[1] In the urban environment, these new technologies are transforming city life and helping pave the way for a more sustainable, resilient and equitable future.

When used effectively, connected devices – like sensors that capture pollution in the air or lights that only turn on when someone is in the room – can produce cost savings,

bolster civic engagement, and strengthen public health and safety. IoT will also drive new economic opportunity and business development.

The expansion of connected devices can also carry significant challenges and risks for cities. Mitigating this risk requires that government play a hands-on role in establishing frameworks and standards, monitoring the expansion of IoT, and maximizing the public benefit derived from these new technologies.

Methodology

These guidelines are the product of extensive research and engagement with stakeholders from the public, private and academic community led by the New York City Mayor's Office of Technology and Innovation. In partnership with a team of consultants, the office surveyed government agencies, offices and departments around the world regarding their use of sensor technologies and other IoT deployments, cataloguing laws, policies, planning documents and contract language to identify commonalities, inconsistencies, opportunities for improvement, and model practices.

Based on this research, more than 450 best practices were identified and consolidated into a preliminary set of guidelines. These guidelines were reviewed by subject matter experts from universities, regulatory and standards bodies, public interest groups, private companies, and city governments around the world before being condensed into the final set of guidelines that appear on this website.

Implementation

These guidelines are intended to serve as a jumping off point for government agencies and partners as we design, install and roll-out new IoT systems using public space or assets.

In some cases, these guidelines may be able to be implemented fairly easily out-of-the-gate. In other cases, new policies, procedures, and resources will need to be developed and may take time. Special circumstances and concerns may also exist for IoT systems and/or data related to public safety, security and law enforcement. As new tools – for example, operational checklists, contract templates, inventories, and sample agreements – are developed, they will be added to this site on a semi-annual basis.

The IoT guidelines are a living document and exist in perpetual "beta" – as such, we will continually collect feedback and monitor their use, making adjustments and additions as necessary so that the guidelines remain as valuable and useful as possible for city government and other stakeholders.

Acknowledgements

The New York City Mayor's Office of Technology and Innovation is grateful for all the individuals and groups who contributed towards the development of these guidelines.

American Civil Liberties Union

Hitachi

IBM

NYC Law Department

American National Standards Institute (ANSI)

City of Amsterdam

City of Valencia, Spain

City of Paris

Columbia University

European Commission, DG CONNECT

Forum Virium Helsinki

GE

International Data Corporation

National Institute of Standards and Technology

NYC Dept. of Citywide Administrative Services

NYC Dept. of Environmental Protection

NYC Dept. of Information Technology and Telecommunications

NYC Dept. of Transportation

NYC Mayor's Office of Data Analytics

NYC Office of the Counsel to the Mayor

NYC Police Department

Qualcomm

SAP

Schneider Electric

Smart Dubai

Tata Consultancy Services

ThingWorx

PARTNER + CONTRIBUTE

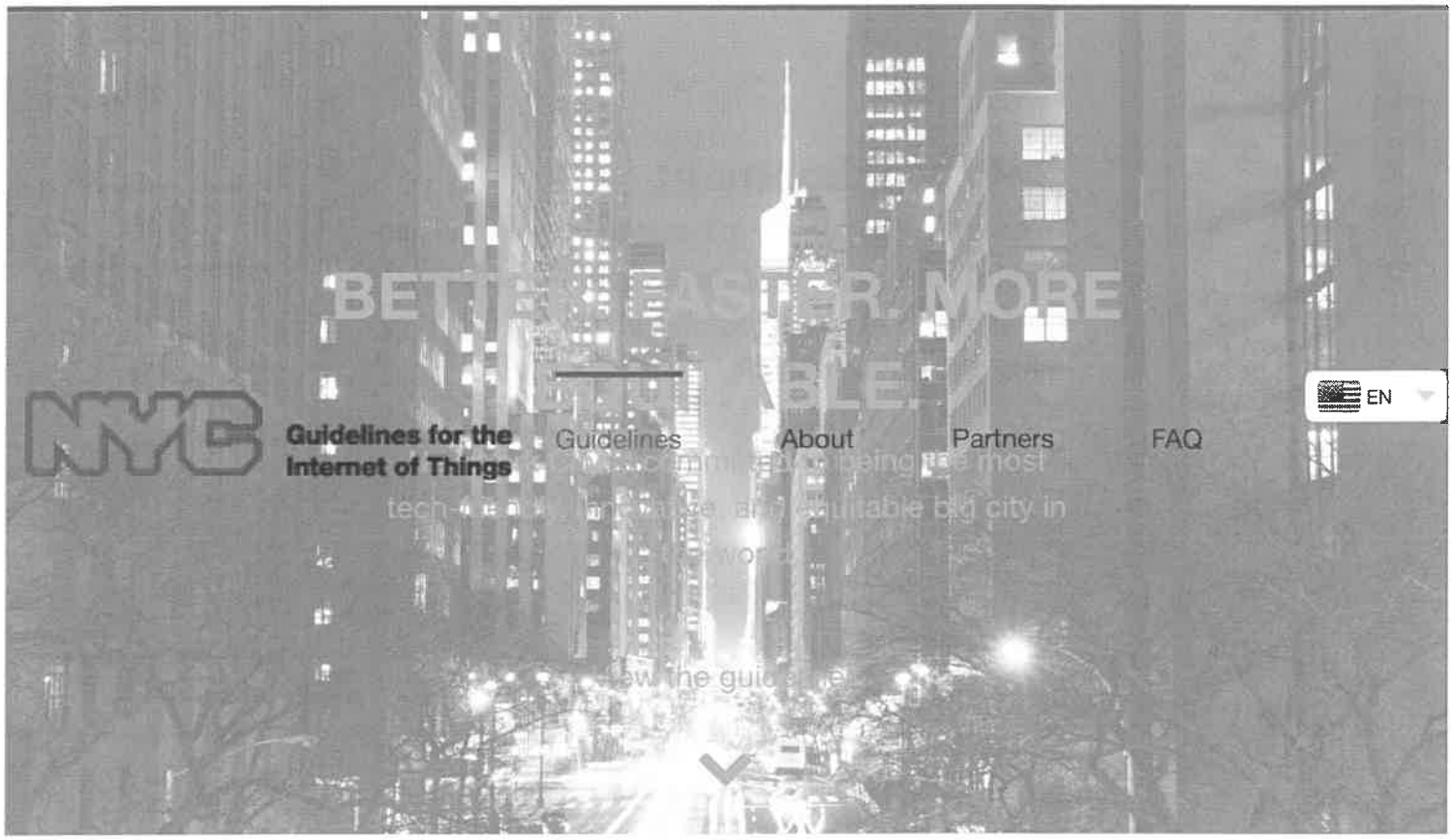
These guidelines are designed to continually evolve and improve over time — we welcome and appreciate all feedback. We also invite cities to join the effort by committing to our guiding principles for the responsible and equitable deployment of smart city technologies. Contact us to learn more.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York



These guidelines provide a framework to help government and our partners responsibly deploy connected devices and IoT technologies in a coordinated and consistent manner. More than 35 leading cities, spanning 11 countries, have now joined New York City in this effort.

1

Privacy + Transparency

When we use new technologies on city streets and in public spaces, we are committed to being open and transparent about the "who, what,

READ MORE >



Data Management

Data is the core of any IoT system. We will ensure that IoT and real-time data is captured, stored, verified, and made accessible in ways that maximize public benefit.

READ MORE >



Infrastructure

To capitalize on the value and benefits derived from public assets, we will deploy, use, maintain and dispose of IoT devices, networks and infrastructure in an efficient, responsible, and secure manner.

READ MORE >



Security

Keeping New Yorkers safe is our top priority. To do so, we are designing and operating IoT systems to protect the public, ensure the integrity of services, and maximize resilience.

READ MORE >



We are committed to streamlining operational processes and ensuring financial, operational, and environmental sustainability to ensure that our city keeps running better and faster.

READ MORE

PARTNER + CONTRIBUTE

These guidelines are designed to continually evolve and improve over time — we welcome and appreciate all feedback. We also invite cities to join the effort by committing to our guiding principles for the responsible and equitable deployment of smart city technologies. Contact us to learn more.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York

1

PRIVACY + TRANSPARENCY

City IoT deployments must protect and respect the privacy of residents and visitors. The City is committed to being open and transparent about the "who, what, where, when, why and how" of data collection, transmission, processing and use.

SHARE THIS GUIDELINE:

1.1: The City should make processes and policies related to IoT and IoT-related data publicly available in an up-to-date, clear and comprehensive manner. IoT principles, guidelines, operational policies and responsibilities should be transparent and made public via a City government website.

1.2: **IoT data should only be collected, transmitted, processed and used** for specified, explicit and legitimate purposes. The purpose of data collection (e.g., a use case such as monitoring air quality), what data is collected (e.g., particulates in the air) and how data is being collected (e.g., pollution sensor on a light pole) should be transparent and made public via a City government website or other public notice.

1.3: **Data and information collected by IoT devices** should be classified and treated accordingly, per the City of New York's Data Classification Policy, as Public, Sensitive, Private or Confidential. All personally identifiable information (PII) should be classified at a minimum as private. All data that is classified as being confidential, or personally identifiable, should be protected from unauthorized use and disclosure.

New York City Data Classification Policy

1.4: **PII should by default be anonymized before being shared** in any way that could make the information publicly searchable or discoverable. Any copies and reproductions must have the same or higher level of classification as the original. Any combinations of data should be reclassified according to the City's Data Classification Policy.

New York City Data Encryption Policy

1.5: **PII data types should have a clearly associated retention policy and disposal procedure**. Sensitive, private or confidential data should be kept for no longer than is operationally necessary or required for the specified, explicit and legitimate purposes.

New York City Digital Media Re-use and Disposal Policy

1.6: **Before any sensitive, private, or confidential data is shared** outside the originating City agency, the agency should ensure that the need cannot be met by using anonymized or aggregated data and that the appropriate

protections are in place to preserve the confidentiality of the data.

1.7: **All public data sets are subject to the NYC Open Data Law** and as such should be freely accessible via the City's Open Data portal.

Related Resources

NYC Open Data Law >

City of New York Data Classification Policy >

NYS Freedom of Information Law >

BACK TO ALL GUIDELINES

DATA MANAGEMENT >

PARTNER + CONTRIBUTE

These guidelines are designed to continually evolve and improve over time — we welcome and appreciate all feedback. We also invite cities to join the effort by committing to our guiding principles for the responsible and equitable deployment of smart city technologies. Contact us to learn more.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York

2

DATA MANAGEMENT

City IoT deployments must protect and respect the privacy of residents and visitors. The City is committed to being open and transparent about the "who, what, where, when, why and how" of data collection, transmission, processing and use.

SHARE THIS GUIDELINE:

2.1: IoT systems (e.g. how data is collected, analyzed and used) should be designed with the use case in mind (e.g. predicting demand for trash pick-up based on data on trash volume, weather and events) to maximize the benefits that can be derived data collection (e.g. routing garbage trucks more efficiently). Where useful, relevant business and historical data from the City or its partners should be made available and utilized by applications.

2.2: The desired measurement from any IoT system (e.g. pedestrian counts) should be collected and categorized as efficiently as possible, using as few steps and/or manipulations as necessary.

2.3: IoT data should be collected and stored according to open standards, contain relevant contextual metadata, be exposed through open, standards-based application program interfaces (APIs), and be provided with software development kits (SDKs) where applicable so it can be easily shared or combined with other data sets.

2.4: IoT data should be archived in a federated way and made accessible throughout the City through a central portal (e.g. the City's open data portal) or a catalogue of documented open APIs unless restricted by existing laws or regulations and/or doing so would compromise privacy or public safety. Data from other systems not operated by the City, such as from a private sector partner or from crowdsourcing, that could provide public benefit can also be provided in this form with the source documented accordingly.

2.5: The City recognizes the use of distinct and sometimes conflicting non-proprietary international, national, or industry standards for data and technology interfaces. In cases where standards conflict, the one that most closely aligns to the use case will be selected.

2.6: Each IoT device data set (e.g. temperature) should be validated and verified (e.g. through redundancy in data collection and/or historical data) and the resulting master copy clearly labeled before it is used, aggregated and/or released. Data should be versioned so that any updated data can be distinguished from the original and/or master copy. The retention and disposal policies for the master copy should be explicitly defined.

2.7: IoT data should be both audited and continuously monitored for accuracy and validity. This process should be automated where possible.

2.8: All data sets (e.g. 311 service requests) should be checked for geographic, social or system-driven bias (e.g. geographic differences in civic engagement) and other quality problems. Any biasing factors should be recorded and provided with the data set and corrected where possible.

Related Resources

NYC Open Data Law >

NYC Open Data Portal >

NYC Open Data Technical Standards Manual (Beta) >

BACK TO ALL GUIDELINES

INFRASTRUCTURE >

PARTNER + CONTRIBUTE

These guidelines are designed to continually evolve and improve over time — we welcome and appreciate all feedback. We also invite cities to join the effort by committing to our guiding principles for the responsible and equitable deployment of smart city technologies. Contact us to learn more.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York

3

INFRASTRUCTURE

IoT devices, networks and infrastructure shall be deployed, used, maintained and disposed of in an efficient, responsible and secure manner to maximize public benefit.

SHARE THIS GUIDELINE:

3.1: **To support citywide coordination** of IoT deployments, City agencies should maintain an inventory of IoT devices that they deploy using a standardized format. City agencies should also maintain an inventory of the public or private assets on which devices are installed and the networks used by these IoT devices including details on the network type (e.g. LTE), security protocol (e.g. WPA), location, service level agreements, and contact information for the network and system operator.

3.2: **The City should accumulate and publish**, via a City government website, public information on IoT systems including but not limited to examples of deployed IoT devices (e.g. air quality sensors) and the different types of public assets (e.g. light poles) on which they are deployed.

3.3: **The City should make public**, via a City government website, a standardized protocol, including points of contact, for requesting access to, and approving use of, City assets for IoT deployments. Where appropriate, the City will detail restrictions on particular types of public assets and/or siting restrictions (e.g. rules for landmark or historic districts).

3.4: **IoT deployments shall, where possible, leverage or repurpose** existing conduit and public assets, maximize energy efficiency, and adhere to sustainable device disposal procedures.

3.5: **The City should leverage existing wireless and fixed networks** where possible and appropriate. Networks for IoT deployments should be selected to best support the specific use case. This should include but is not limited to ensuring appropriate security protocols, bandwidth, pricing models, and service level agreements (SLAs).

3.6: **All IoT devices and network equipment installed by the City**, on the City's behalf, or on City property should have clear site license agreements and established terms of service governing who is responsible for ongoing operations, maintenance, and the secure disposal of equipment. IoT devices and network equipment should be labeled clearly with the name and contact information for the responsible party.

3.7: **Public assets should be instrumented in an orderly manner** that minimizes clutter and allows for ease of access for replacement, repair and addition of new equipment or devices. If new conduit is being installed using public assets (e.g. to access rooftop of public buildings) or using public right-of-way (e.g. in City streets), location details must be

filed with the responsible agency and use of the conduit should not be restricted to one party.

3.8: **IoT systems should be designed to maximize resiliency** in the event of a natural disaster (e.g. severe flooding) or other emergencies (e.g. electrical outages). Critical systems should have established emergency response plans to ensure the appropriate continuity of service.

Related Resources

NYC Department of Transportation Street Design Manual >

NYC Public Design Commission Street Design Guidelines >

BACK TO ALL GUIDELINES

SECURITY >

PARTNER + CONTRIBUTE

These guidelines are designed to continually evolve and improve over time — we welcome and appreciate all feedback. We also invite cities to join the effort by committing to our guiding principles for the responsible and equitable deployment of smart city technologies. Contact us to learn more.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York



SECURITY

IoT systems should be designed and operated with security in mind to protect of the public, ensure the integrity of services, and be resilient to attacks.

SHARE THIS GUIDELINE:



4.1: **IoT systems should be designed with an explicit focus** on minimizing security risks (e.g. unauthorized operation or hacking, system faults, tampering, and environmental risks), limiting the potential impact from a security breach (e.g. the release of personally identifiable information), and ensuring that any compromises can be quickly detected and managed.

4.2: **IoT systems should utilize established security frameworks**, where possible, and ensure communication

between components is tightly constrained.

4.3: **Identity and access management controls should be in place** to ensure that the right people have access to systems, networks, and data at the right time. Users with access to IoT systems should be identified and authenticated. Identification should be to the individual and not to the role.

4.4: **All data should be protected in transit and at rest**, and systems should be secured against unauthorized access or operation. Data storage mechanisms must not be easily removed from devices and systems must not have vulnerable external interfaces (e.g. unsecured USB ports).

4.5: **All partners utilizing public assets and/or networks** for IoT deployments should adhere to the principles and guidelines set by the City. The City has the right to restrict or revoke access to assets, devices, and public networks to protect the public interest and public safety.

4.6: **The City and its partners should engage** in both audit-based and continuous monitoring to ensure that systems are working and that devices have not been compromised.

4.7: **Responsibilities related to security monitoring and the protection** of IoT systems should be clearly defined. In the event of a breach, public and private sector entities will be required to comply with the City's breach disclosure and notification requirements.

Related Resources

NYC Department of Information Technology & Telecommunications Vendor Security Policies >



OPERATIONS + SUSTAINABILITY

All IoT deployments should be structured to maximize public benefit and ensure financial, operational, and environmental sustainability.

SHARE THIS GUIDELINE:



5.1: **Demonstrated need, business case, and public benefit** (e.g. economic, social, and environmental outcomes) should be required prior to deployment of any new IoT devices or solutions. In addition, proof of concept should be required prior to citywide deployments.

5.2: **Prior to deployment, the City and its partners shall identify** all stakeholder and user groups (e.g. community

residents and city employees) that will be impacted by the IoT solution and establish feedback mechanisms and methods of engagement for these groups. Before and during deployment, the City and its partners should also check for and address biases in the IoT solution (e.g. information asymmetries) that may result in unintended consequences (e.g. inequitable service delivery).

5.3: **The City shall prioritize access to its assets and public networks** for IoT device deployments that are distributed in an equitable manner and have the greatest public benefit. Public-private partnerships and business models that offset costs or generate revenue in ways aligned with greatest public benefit are encouraged but must be closely evaluated for risk.

5.4: **All projects and associated contracts or agreements** should outline the "who, what, where, when, why and how" of the implementation, operations, risk management, knowledge transfer, and maintenance of IoT systems. This should include clear definitions related to system and data ownership and responsibilities.

5.5: **Solutions shall be designed to be flexible and responsive** to evolving needs. Agreements should enable the addition of new functions and update of components over the life of the agreement at a fair and transparent cost.

5.6: **Performance metrics should be maintained for solutions.** Agreements should specify intended outcomes of a solution and levels of service and provide for penalties, modifications, or terminations of the agreement in the event that the solution does not perform.

5.7: **The City and its partners should reuse infrastructures and components** where possible, leverage citywide contracts or agreements, and develop solutions collaboratively among agencies to avoid duplicating existing solutions or functions and extract the greatest value from investments.

5.8: All components of a solution should be implemented in a modular manner, prioritizing open standards where possible, to ensure interoperability and prevent dependency on a single vendor.

Related Resources

OneNYC: The Plan for a Strong and Just City >

One City: Built to Last >

BACK TO ALL GUIDELINES

PRIVACY + TRANSPARENCY >

PARTNER + CONTRIBUTE

These guidelines are designed to continually evolve and improve over time — we welcome and appreciate all feedback. We also invite cities to join the effort by committing to our guiding principles for the responsible and equitable deployment of smart city technologies. Contact us to learn more.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York

PARTNERS

More than 35 cities spanning 11 countries, along with the Council of Global City Chief Information Officers, have launched a new initiative focused on ensuring responsible and equitable deployment of smart city technologies.

The effort, led by the City of New York, has three primary goals: **(1)** provide a common framework to help governments develop and expand policies and procedures related to the Internet of Things; **(2)** ensure openness and transparency regarding the use of public space or assets for smart city technologies; and **(3)** advance the public dialogue about how government, the private sector and academia can collaborate to ensure these technologies are used in a way that maximizes public benefit.

> Download the 9/26/16 press release here (.pdf)
> Download a sign-on form for cities (.doc)

[1]

When we use new smart technologies on city streets and in public spaces, we are committed to being open and transparent about the "who, what, where, when, and why" for any data or information being collected and used.

[2]

To capitalize on the value and benefits derived from public assets, we will deploy, use, maintain and dispose of IoT devices, networks and infrastructure in an efficient, responsible, and secure manner.

[3]

We will ensure that IoT and real-time data is captured, stored, verified, and made accessible in ways that maximize public benefit.

[4]

We will design and operate IoT systems to protect the public, ensure the integrity of services, and maximize resilience.

[5]

We are committed to streamlining operational processes and ensuring financial, operational, and environmental sustainability to ensure that our city keeps running better and faster.

Partner Cities

The following cities have committed to a common set of guiding principles that emphasize privacy, security, sustainability, resilience, equity and efficiency in their use of these technologies:

Atlanta, Georgia, U.S.A.

Austin, Texas, U.S.A.

Birmingham, England, United Kingdom

Boston, Massachusetts, U.S.A.

Bradford MDC, England, United Kingdom

Bristol, England, United Kingdom

Canberra, Australia

Cambridge, Massachusetts, U.S.A.

Florence, Italy

Greenville, South Carolina, U.S.A.

Kansas City, Missouri, U.S.A.

Leeds, England, United Kingdom

Limerick, Ireland

Los Angeles, California, U.S.A.

Milton Keynes, England, United Kingdom

New York, New York, U.S.A.

Osaka, Japan

Palo Alto, California, U.S.A.

Portland, Oregon, U.S.A.

San Antonio, Texas, U.S.A.

San Diego, California, U.S.A.

San Francisco, California, U.S.A.

Seattle, Washington, U.S.A.

Spokane, Washington, U.S.A.

Stockholm, Sweden

Tel Aviv, Israel

Valencia, Spain

Vancouver, British Columbia,

Chicago, Illinois, U.S.A.

Dallas, Texas, U.S.A.

Dublin, Ireland

Pittsburgh, Pennsylvania

District of Columbia, U.S.A.

Wellington, New Zealand

JOIN THE EFFORT

Interested in becoming a partner? Contact us if you would like to adopt these principles in your city and connect with other municipal leaders focused on smart city deployments.

CONTACT US

smart + equitable city Guidelines

SHARE THIS SITE:

Copyright 2017 The City of New York