(d)2 – Privacy Policy Update

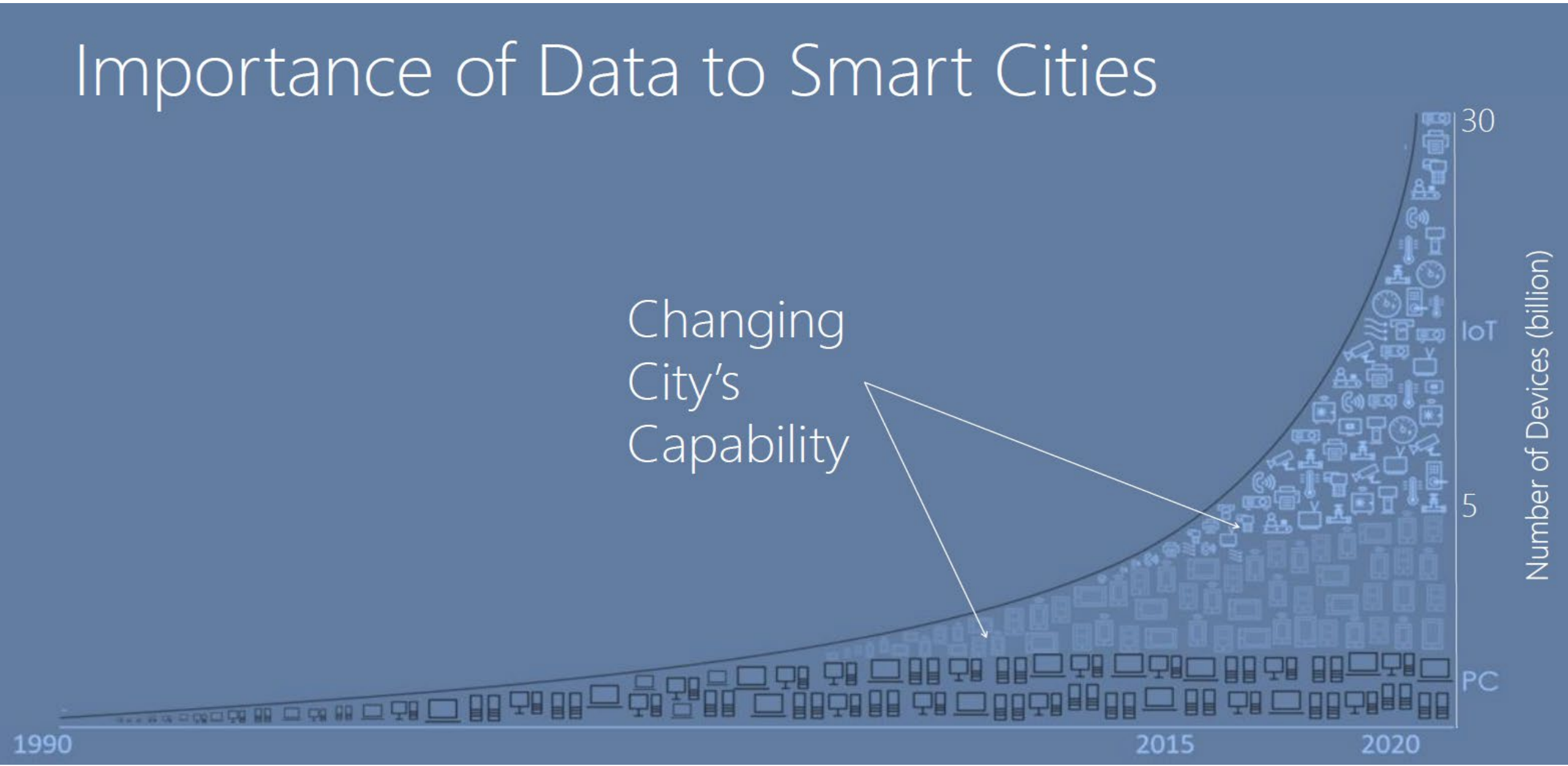
Smart Cities and Service Improvements Committee

November 5, 2020

Andrew Ehrich, Assistant to the City Manager, City Data Analytics Lead

Marcelo Peredo, City Information Security Officer

Why is Digital Privacy Important to San José?



Why is Digital Privacy Important to San José?

PII = Personally Identifiable Information

FIVE CATEGORIES OF PII

Personal Data

- Name, address, birthday, email

Sensitive Data

- Biometrics, genetics, race, ethnicity, religion, politics

Image Data

- Pictures or photographs

Recording Data

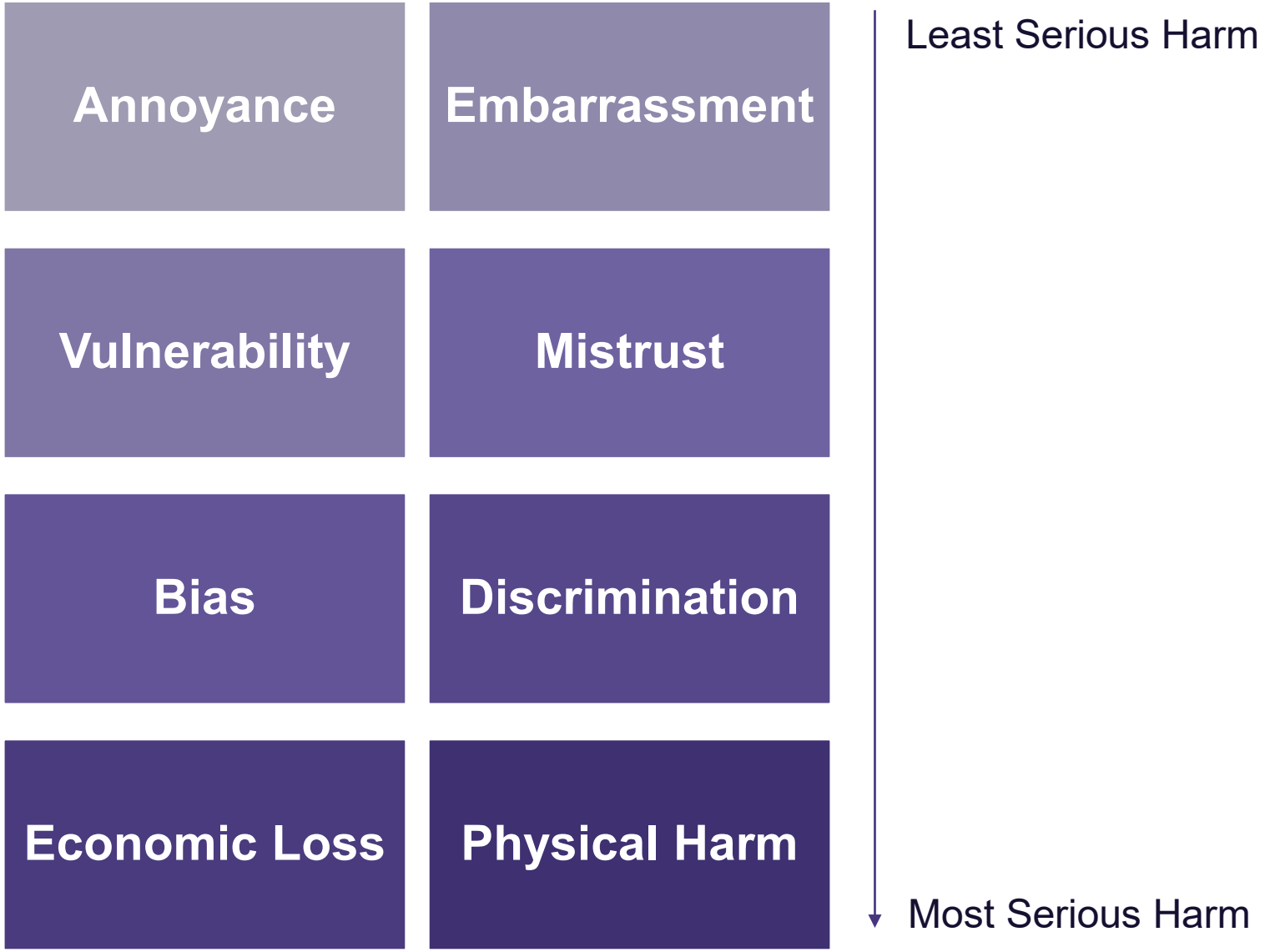
- Audio, video

Geolocation Data

- Device data, vehicle data

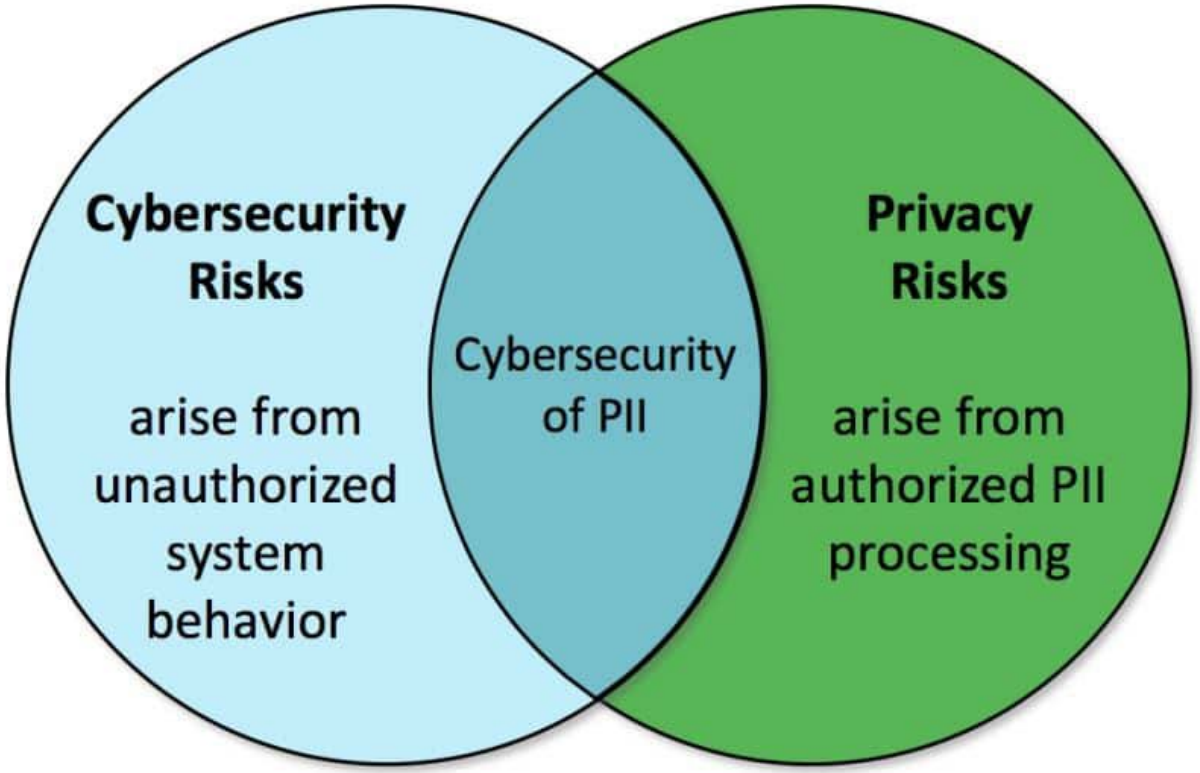
Why is Digital Privacy Important to San José?

Adverse Effects of Privacy Violations:



Why is Digital Privacy Important to San José?

Protecting privacy means addressing both unauthorized *and* authorized data access



Why is Digital Privacy Important to San José?

~10 Million Records with PII

50% Increase of attacks on State and Local Governments*

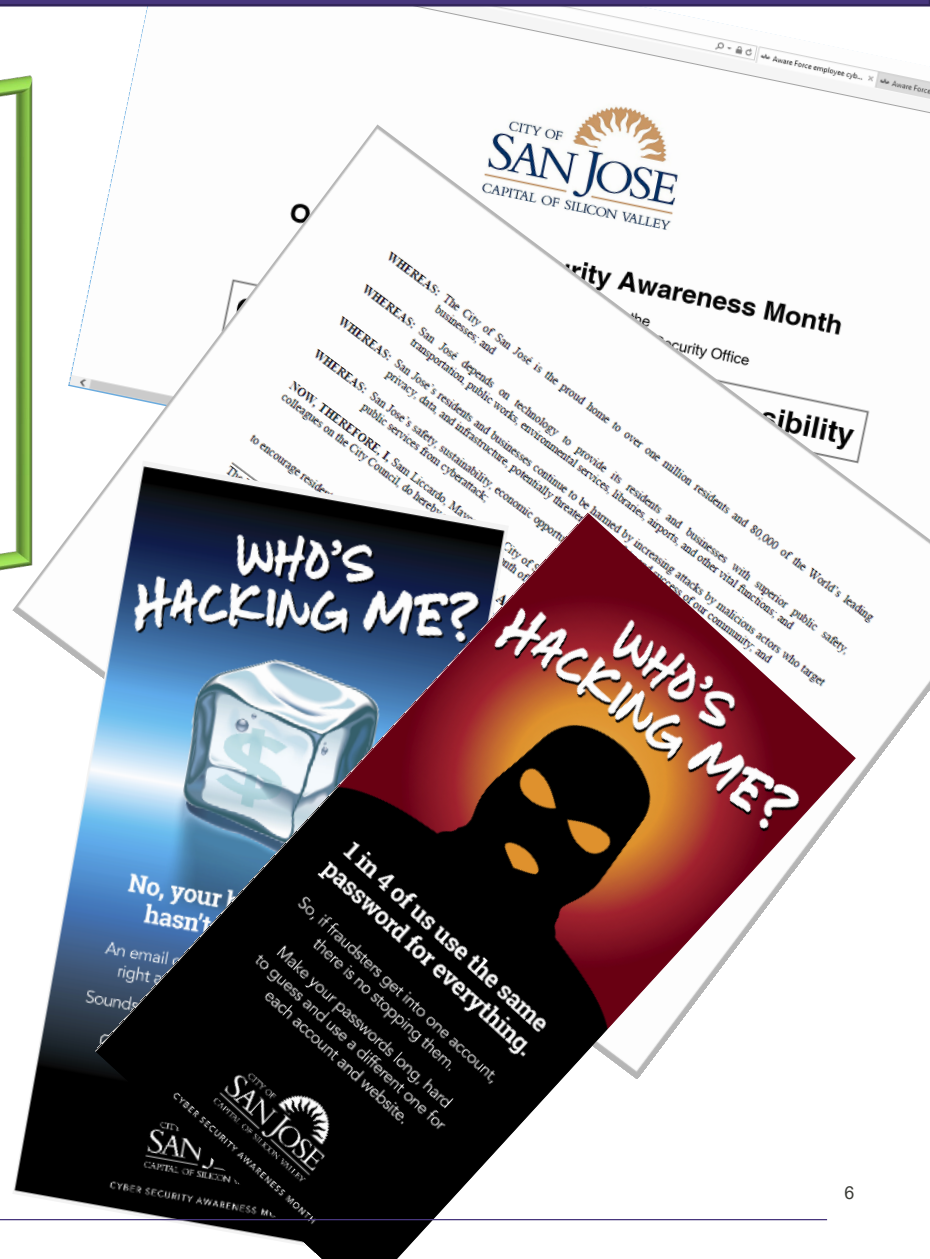
Significant costs in repairs

Operationalize Privacy Policy

Risk ↑ = Threat ↑ * Vulnerabilities ↑ * Impact * Likelihood ↑

The risk has changed due to COVID-19 targeting home-based workers with:

- Phishing scams
- Malware
- Social Engineering
- Impersonations



* BlueVoyant State and Local Government Security Report – August 2020

Why is Digital Privacy Important to San José?

CURRENT CYBERSECURITY APPROACH

	Function	Category
What processes and assets need protection?	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management[1.1]
What safeguards are available?	Protect	**Identity Management, Authentication and Access Control**[1.1]
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	Recover	Recovery Planning
		Improvements
		Communications

PRIVACY PRINCIPLES AND FUTURE POLICY

Privacy Governance	Privacy Governance to maintain optimal Policy and procedural efficiency.
Collect and Keep Only What Is Needed	Ensure that we only collect what we need and not more on every system we own and operate. Thus reducing the footprint of Privacy Data.
We Give Control Over Your Data	We provide information about our Security Practices to the public when they request it. Respond to privacy inquiries.
Open and Transparent	Allow for people to request information regarding their data. Respond to individual requests.
Only Share What is Needed	Ensure that controls are in place when we share data.
Assess Existing Systems	Ensure we conduct regular Privacy Impact Analysis on our systems to determine the level or risk and mitigation strategies.

Our North Star

Why Have A Privacy Policy?

A Citywide Privacy Policy is crucial **to safeguard and protect the public's trust** as the City increasingly **adopts new processes and technologies** to better serve our residents.

WHEN WE LAST LEFT OUR HEROES…

When We Last Left Our Heroes…

City of San José Privacy Principles

Approved by City Council, Sep 2019

WE VALUE PRIVACY: We affirm that privacy is an inherent human right. San José commits to fully evaluating risks to your privacy before collecting, using, or sharing your information.

WE COLLECT ONLY WHAT WE NEED: We collect only what is required to provide and improve city services and comply with the law. We seek community input about what information is used and collected.

WE ARE OPEN AND TRANSPARENT: We are transparent about what information we collect, why we collect it, and how it is used. We commit to being open about our actions, policies, and procedures related to your data. We make our policy documents publicly available and easy to understand.

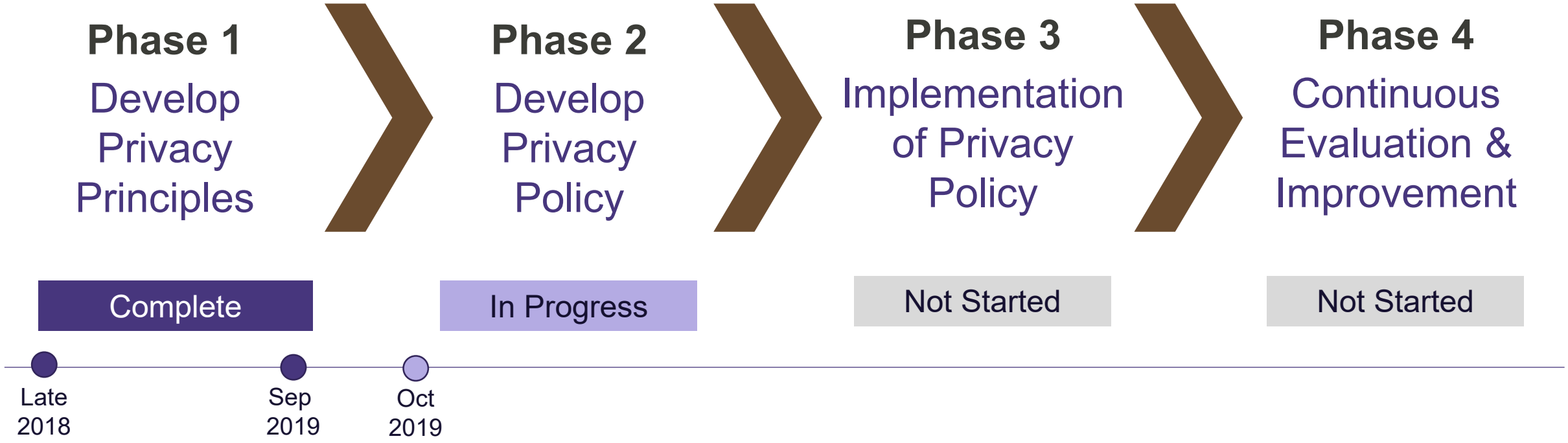
WE WILL GIVE YOU CONTROL OVER YOUR DATA: We will provide you with the information to make an informed decision about sharing your data. We have clear processes that ensure data accuracy and provide you visibility into what data the city has collected from you.

WE SHARE ONLY WHAT WE NEED: We anonymize your information before we share it outside the city, except in very limited circumstances. Business partners and contracted vendors who receive or collect personal information from us or for us to deliver city services must agree to our privacy requirements.

WE DESIGN FOR PRIVACY AND SECURITY: We integrate privacy and security into every aspect of our designs, systems, and processes. We commit to updating our technology and processes to effectively protect your information while under our care. We follow strict protocols in the event your information is compromised.

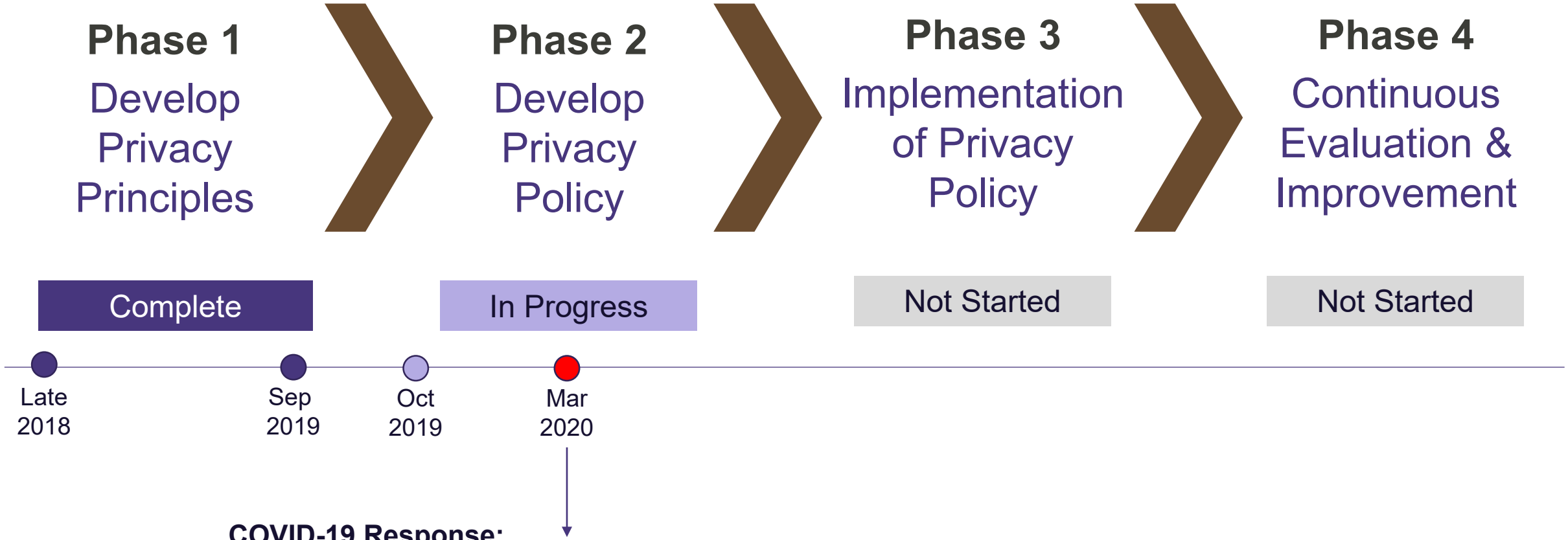
When We Last Left Our Heroes…

From Privacy Principles to Privacy Policy:



When We Last Left Our Heroes…

From Privacy Principles to Privacy Policy:

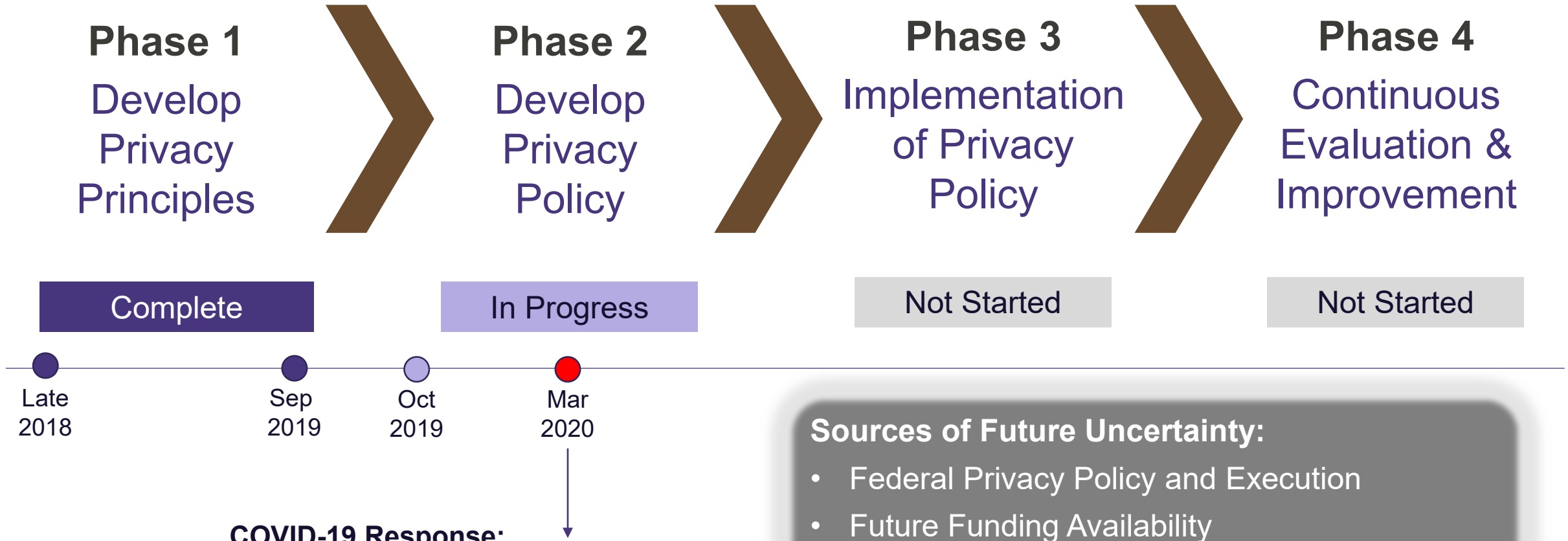


COVID-19 Response:

- Privacy Work Paused
- Privacy Staff Deployed to EOC
- Privacy Staff Not Funded for 2020-2021

When We Last Left Our Heroes…

From Privacy Principles to Privacy Policy:



COVID-19 Response:

- Privacy Work Paused
- Privacy Staff Deployed to EOC
- Privacy Staff Not Funded for 2020-2021

Sources of Future Uncertainty:

- Federal Privacy Policy and Execution
- Future Funding Availability
- Dynamic Area of Policy, Constantly Evolving

PRIVACY POLICY CHALLENGE

How might San José accelerate the development and implementation of a Citywide privacy policy and minimize future rework in an environment of significant policy, technological, and funding uncertainty?

General Data Privacy Regulations (GDPR)

- Human-rights based privacy policy adopted by European Union in May 2016 and effective as of May 2018
- Formally or informally adopted by public and private sector organizations worldwide
- Consists of:
  - **Privacy principles** based on human rights that closely align with the City of San Jose's recently approved privacy principles;
  - **Articles** that comprise the legislation including the need to conduct a privacy impact assessment on any "at risk" technology that might process PII; and
  - **Mandatory governance structure** including a Data Privacy Officer per any organization that processes PII
- City intends to model our Policy after this structure and case studies from other cities

General Data Privacy Regulations (GDPR)

KEY OPERATIONAL ELEMENTS FOR A MUNICIPALITY:

- **Risk Assessment** – assigns the degree of risk that a project, system, or technology processes personal data and could be at risk of violating the principles and articles.
- **Data Protection Impact Assessment (DPIA)** – when there is high risk to the individual rights of the data subject or where new technologies are used, a DPIA is created to identify risks and if necessary, identify corrective action.

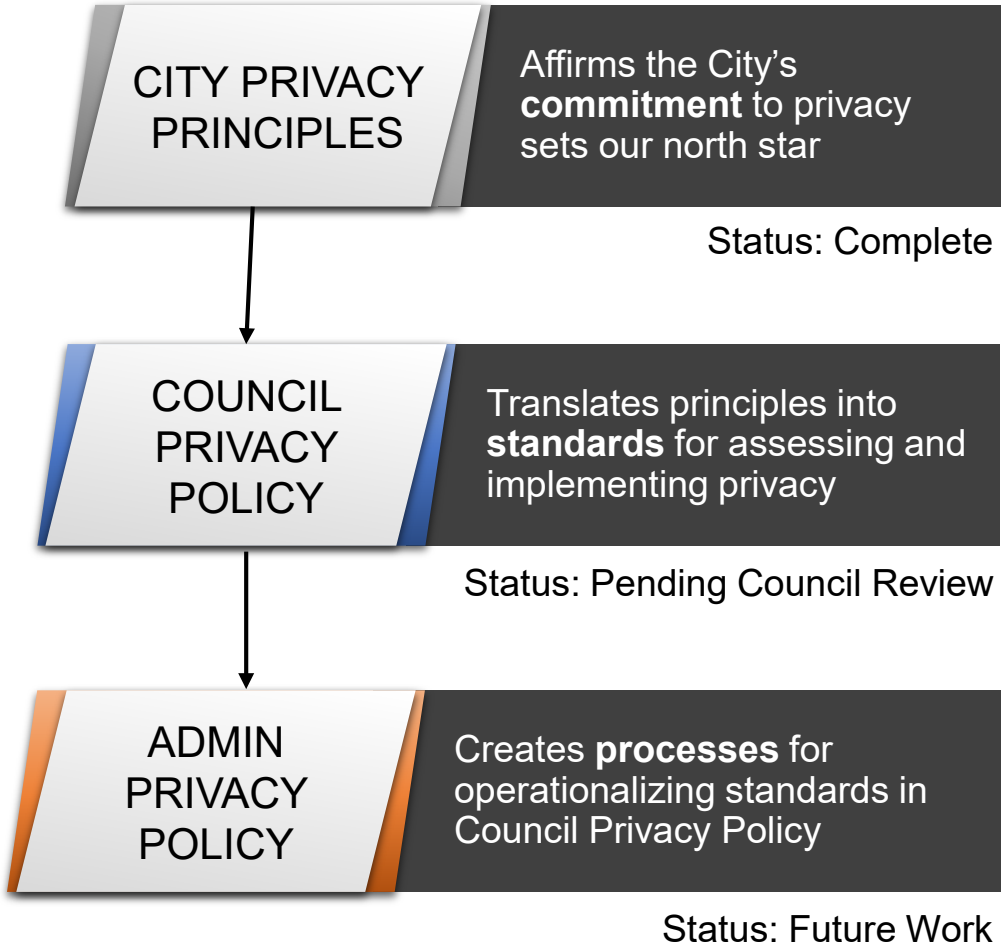
General Data Privacy Regulations (GDPR)

BENEFITS FOR SAN JOSE:

- **Alignment with San José's Privacy Principles –** implementing a policy framework that protects privacy as a human right;
- **Accelerated policy development and implementation –** leveraging best practices and lessons learned from other leading institutions;
- **Minimized policy rework –** aligning San Jose's privacy policy with the ongoing evolution of the world's most comprehensive privacy policy; and
- **Leading the nation -** advancing the City of San Jose's leadership role in smart city policy development including privacy, 5G next generation network deployments, and digital equity.

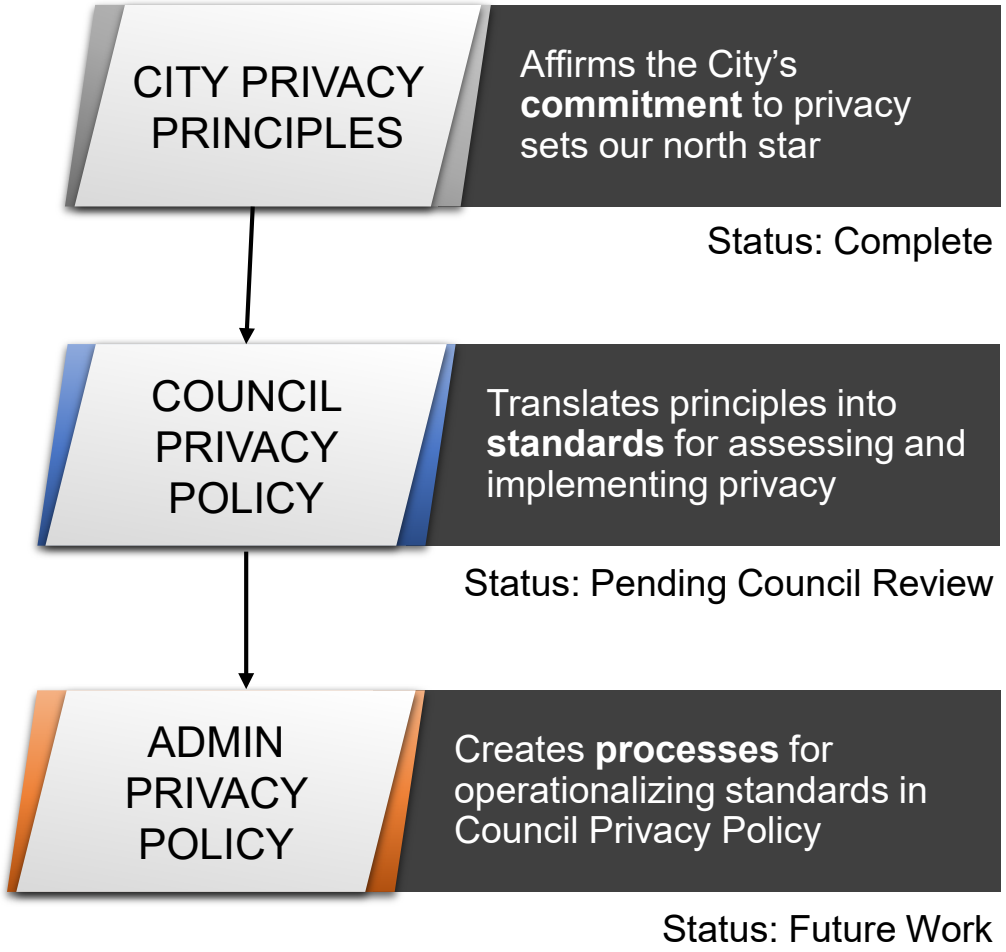
Adapting GDPR to San José

GOVERNANCE FRAMEWORK



Adapting GDPR to San José

GOVERNANCE FRAMEWORK

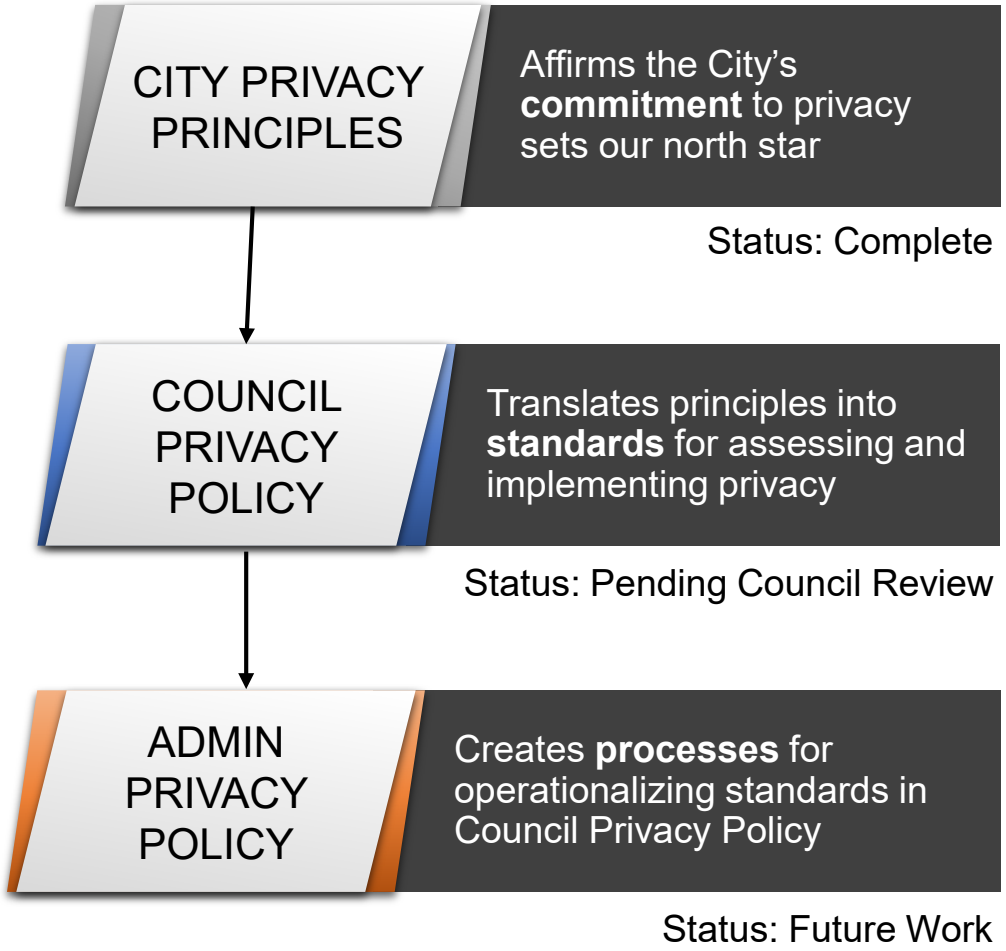


Inputs to Council Digital Privacy Policy

- **Case studies** of other cities and countries who have modeled privacy programs on GDPR
- **Privacy Advisory Task Force**, comprised of community leaders from a variety of sectors
- **Stakeholder engagement** and outreach to City departments

Adapting GDPR to San José

GOVERNANCE FRAMEWORK

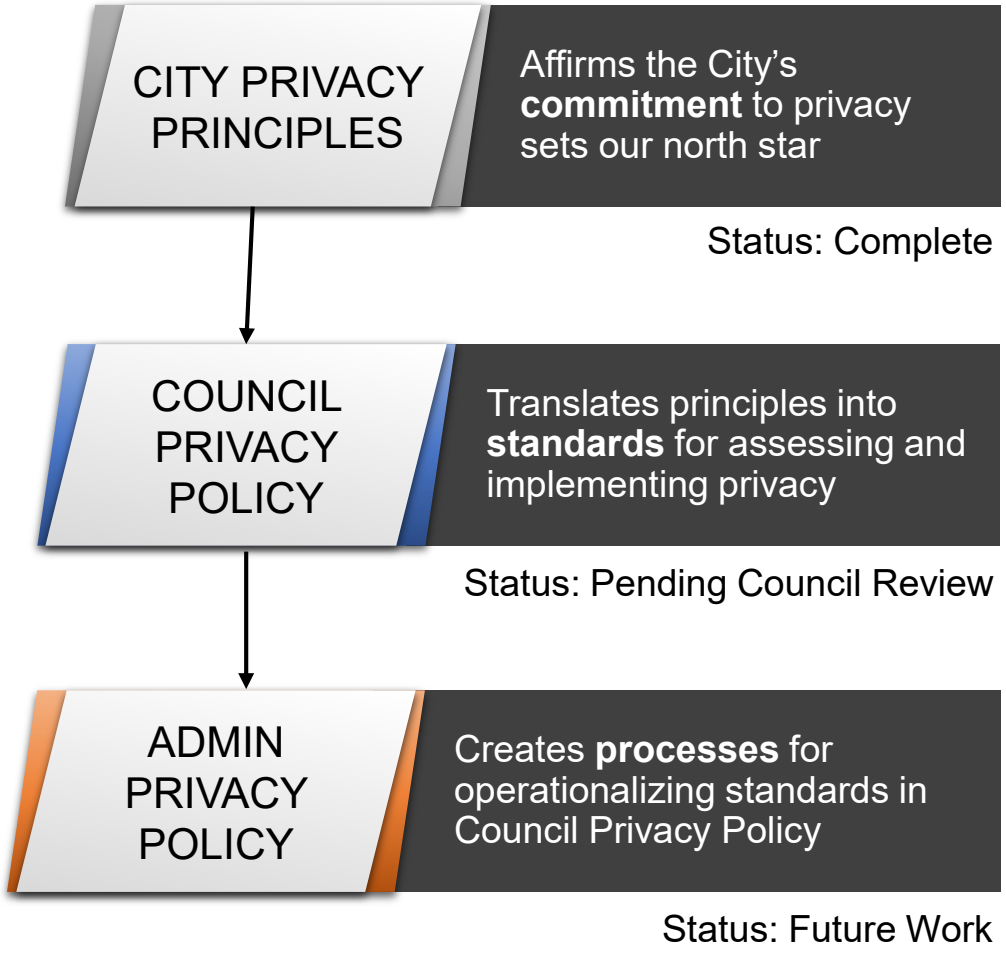


Key Items in Council Digital Privacy Policy:

- Defines clear categories of personally identifiable information (PII) covered by the policy
- Creates standards to assess privacy risk, applicable to City departments, offices, vendors, and contracts
- Directs creation of GDPR-based procedures for prioritizing and assessing privacy risk
- Creates initial digital privacy policy governance and authority within the City Manager's Office to carry out Council direction

Adapting GDPR to San José

GOVERNANCE FRAMEWORK



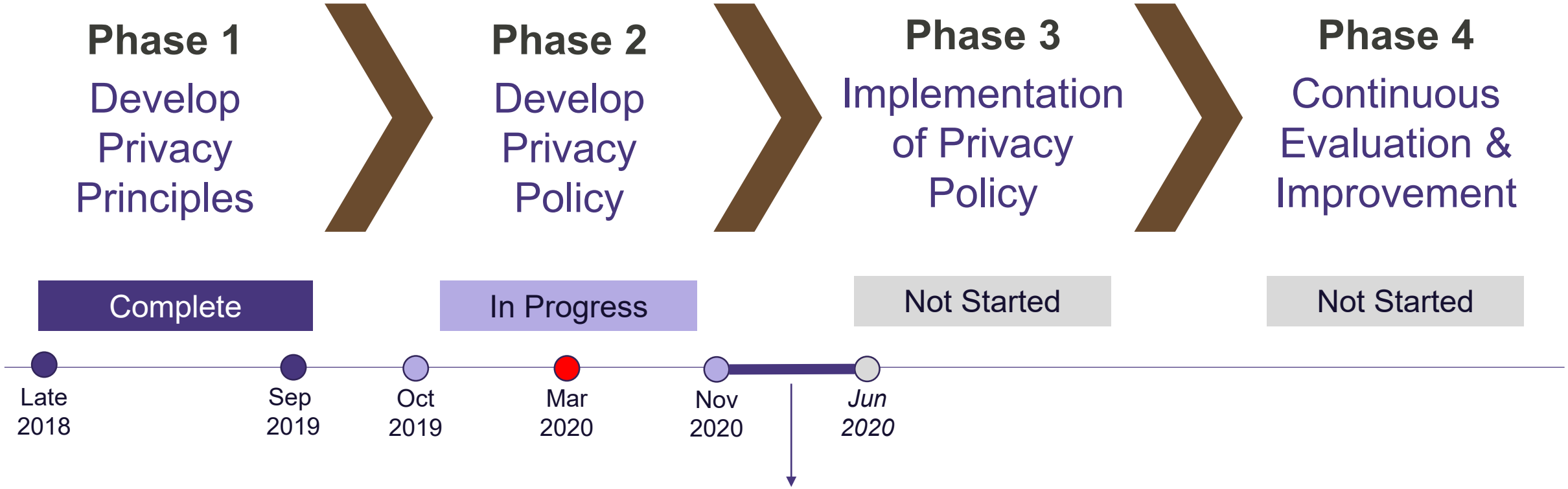
Standards in Council Digital Privacy Policy:

- **Notice:** Regarding collection or use of PII
- **Retention**: Keeping data only as long as needed
- **Minimization**: Anonymize or de-identify if possible
- **Accountability:** In case of breach
- **Accuracy**: Human oversight of predictive systems
- **Sharing:** Enable only safe data sharing
- **Equity:** Protect against discrimination and bias

NEXT STEPS: IMPLEMENTATION

When We Last Left Our Heroes…

From Privacy Principles to Privacy Policy:



Implementation Planning and Budgeting:

- Staffing and Funding Assessment
- Initial Planning for GDPR Processes
- Initial Design of Citywide Privacy Governance
- Community Outreach and Education

Implementation Planning Priorities

- **Initial planning and design** of Risk Assessments and Data Privacy Impact Assessments;
- **Initial design of privacy governance** to enable clear decisions and action based on GDPR assessment processes; and
- **Community outreach and education in three languages** with nonprofit partner CivicMakers to more deeply educate residents, understand community concerns, and inform design of future implementation.

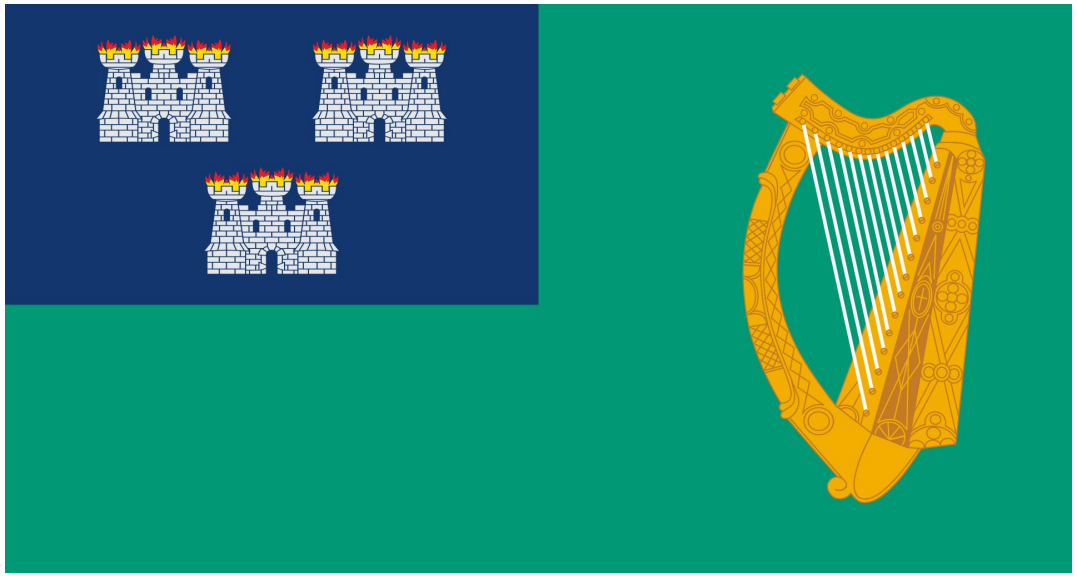
CivicMakers

Comparative Case Studies

IMPLEMENTATION TIMELINES AND FUNDING

City of Seattle

- Program Established 2015
- 4.0 Full-Time Staff, Plus Departmental Resources



- Estimate 8 Years to Full GDPR Compliance
- 4.0 Full-Time Staff, Plus Departmental Resources

Privacy Policy Implementation – Potential Levels of Service

	Reactive Privacy Posture *Current Funding*	**Responsive Privacy Posture** *Partial Funding*	**Proactive Privacy Posture** *Full Funding*
Description	Assess, secure, and respond to only a limited number (estimated 10% coverage) of high-risk systems Minimal capacity to adapt to new statutory privacy frameworks	Assess, secure, and respond to some (estimated 50% coverage) of privacy-relevant systems and requests Reasonable capacity to adapt to new statutory privacy frameworks Advise departments with expertise upon request	Assess, secure, and respond to almost all (estimated 90% coverage) privacy-relevant systems and requests Full capacity to adopt new privacy frameworks Support departments with expertise, training, and toolkit resources Invest in innovative citywide technology and processes to protect privacy

Privacy Policy Implementation – Potential Levels of Service

	Reactive Privacy Posture *Current Funding*	**Responsive Privacy Posture** *Partial Funding*	**Proactive Privacy Posture** *Full Funding*
Assess	• 0.1 FTE (City Data Lead) • $45K - Already Budgeted	• 0.1 FTE (City Data Lead) • **1.0 FTE (Privacy Analyst)** • **$25K - Ongoing Assessment**	• **1.0 FTE (Chief Privacy Officer)** • **1.0 FTE (Privacy Analyst)** • **$25K - Ongoing Assessment**
Secure	• 0.25 FTE (ITD Cybersecurity)	• **0.75 FTE (ITD Cybersecurity)** • **$100K - Privacy Technology**	• **1.25 FTE (ITD Cybersecurity)** • **$200K - Privacy Technology**
Respond	• 0.1 FTE (City Data Lead) • $45K - Community Engagement	• 0.1 FTE (City Data Lead) • **1.0 FTE (Privacy Analyst)** • **$25K - Community Engagement**	• **0.5 FTE (Privacy Attorney)** • **1.0 FTE (Privacy Analyst)** • **$25K - Community Engagement**
Est. New Funding	• None	• 2.5 FTE • $150,000 Non-Personnel • **Est. $500,000 Total**	• 4.5 FTE • $250,000 Non-Personnel • **Est. $1,000,000 Total**

Timeline and Next Steps

- **Report to Smart Cities Committee** – By July 2021
  - Review implementation planning progress
  - Review any evolution in federal, state, or international approach to privacy
  - Receive feedback on staffing and funding options for 2021-2022 implementation
- **2020-2021 Budget Process**
  - Present funding options for Council consideration in 2021-2022 Operating Budget

Our North Star

Why Have A Privacy Policy?

A Citywide Privacy Policy is crucial **to safeguard and protect the public's trust** as the City increasingly **adopts new processes and technologies** to better serve our residents.

(d)2 – Privacy Policy Update

Smart Cities and Service Improvements Committee

November 5, 2020

Andrew Ehrich, Assistant to the City Manager, City Data Analytics Lead

Marcelo Peredo, City Information Security Officer

Implementation Planning Priorities

Phase 2 Deliverables **Presented Sep 2019**	***Status*** **Pending Council Action**	**FY20-21** **Planning Priority**
▪ *Citywide Privacy Policy*	**Complete**	-
▪ *Citywide Data Retention Schedule*	**Complete**	-
▪ *Privacy Impact Assessment Process*	**In Progress**	**Yes**
▪ *Training Framework for City Departments*	-	-
▪ *Master List of Sensing Technologies*	**Complete**	-
▪ *Sustainable Privacy Governance Model*	**In Progress**	**Yes**
▪ *Community and Stakeholder Engagement*	**In Progress**	**Yes**