BTS-2.19 Cloud Services Governance

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Search Code, Charter, Policy

Keywords

Search

Policy category: Technology Services

Policy number: 2.19

Purpose

The information technology industry continues to shift service offerings from on-premises based systems to cloud-based services. The City of Portland is adopting cloud-based services in line with industry trends. Due care and due diligence of City information and Public Records requirements is a mandate of BTS to "ensure confidentiality, integrity and availability of electronic information…"

Administrative Rule

This policy outlines the requirements for Cloud Services use by the City of Portland and its Authorized Users per BTS-2.01. This policy applies to all City of Portland bureaus, divisions, entities and Authorized Users. Both internal City Cloud deployments (Private Cloud) and external partnerships (Public Cloud) must comply with this policy per PCC 3.15.090(B).

Cloud, or 'hosted services' take many forms, including:

IaaS – Infrastructure as a Service – The Cloud Service Provider (CSP) provides the hardware in their data center. The Cloud Consumer manages the configuration and operation of operating systems (such as Windows), databases, storage, applications, security and application use.

PaaS – Platform as a Service – The CSP provides, configures and manages the hardware, operating systems, storage and database platforms. The Cloud Consumer configures and manages the use of the platforms, application's security and use.

SaaS – Software as a Service – The CSP provides, configures and manages the hardware, operating systems, databases, storage and applications. The Cloud Consumer manages the use of the application and may manage some aspect of application configuration and authorization of user access to the applications.

FaaS – Functions, or applications, as a Service, such as AWS (Amazon Web Services) Lambda, Kubernetes, Docker, etc.

Other - Any other cloud-based service, application, media, platform, or data repository.

Cloud Services

1. Use of Cloud Services must follow all other applicable BTS Admin rules (Technology Services | Portland.gov), City Procurement Rules (Chapter 5.33 Goods and Services | Portland.gov) and any other applicable City of Portland rules.
    A. Early engagement of BTS Information Security ensures Cloud Services align with applicable regulatory, City information security, privacy, data classification and governance requirements.

2. IaaS and PaaS
    A. For IaaS and PaaS, Bureau of Technology Services (BTS) will manage Azure, Amazon Web Services (AWS) and any other cloud provider infrastructure, platform configuration and Authorized User account access.

    B. Billing for these and other IaaS and PaaS Cloud Services will be managed through BTS. Bureaus will be responsible for monitoring and managing use of metered Cloud Services and associated costs. Billing is the responsibility of the individuals appointed as accountable for each bureau, division, or entity to monitor their data use and billing.

    C. Adjustments to Cloud Service subscriptions will be made through BTS.

3. SaaS and FaaS
    A. Use of and subscription to SaaS/FaaS must be auditable, discoverable, and capable of having information and cyber risk assessed.

    B. Cloud Services providers shall follow all applicable industry control best practices for all critical security updates and patches.

    C. SaaS/FaaS vendors must allow BTS to routinely audit their security posture or provide annual third-party auditor documentation of their security posture, which should be equivalent to a SOC 2 Type II security assessment.

    D. Cloud Services providers are expected to cooperate with City and Law Enforcement investigations of service and data availability, integrity and security, including suspected compromise or breach of data or services.

   E. Non-Standard SaaS or FaaS applications are subject to the BTS Exception Process.

4. Internal and external Cloud Services must leverage the City's Single Sign On (SSO) and Identity and Access Management (IdAM) platforms.
   A. Multi-Factor Authentication must be enabled for access to Cloud Services.

   B. Exceptions will be evaluated during the contracting process.

Legal and Contracts

1. The City's use of Cloud Services must comply with all applicable federal, state, and local laws and regulations.
   A. City Data must be always located within the United States, whether at rest, in transit, or otherwise, except as provided by BTS authorized exception.
2. All contract awards for Cloud Services must comply with City procurement code PCC 5.33 and 5.68, as applicable.
3. All contracts for Cloud Services must be submitted to the City Attorney's Office for review and approval as to form, regardless of value as required by PCC 3.10.030(B).

Data Governance, Privacy and Security

1. Bureaus managing Cloud Services data repositories must align data governance, ownership, privacy and security with City standards and requirements. (See References)
2. Bureaus must comply with City data retention policy and schedules as determined by the Auditor's Office.
   A. BTS can assist in configuring compliant IaaS and PaaS services. Also see Exit Strategy below.
3. Cloud Services containing sensitive data types are subject to additional compliance requirements, including but not limited to the following: Payment Card Industry data (PCI), Personally Identifiable Information (PII), Federal Tax Information (FTI), Criminal Justice Information Services data (CJIS), and Personal Health Information (PHI).
4. City-specific data types (Public, Restricted and Confidential) must be stored, accessed and transmitted in accordance with applicable City data governance polices, and as defined in BTS-2.18 Information Classification & Protection.

Exit Strategy

1. Cloud Services and contracts should be developed with an exit strategy for disengaging from the vendor. The City must determine how data can be recovered from the vendor and archived, if

necessary, or deleted with confirmation by the vendor, at the time of contract termination or expiration.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

1. BTS Technology Definitions – https://www.portlandoregon.gov/...
2. City of Portland Security Standards
3. (BTS) Technology Standards Directory (and Acronyms) – https://www.portlandoregon.gov/...

History

Ordinance No. 179999, passed by City Council March 15, 2006, and effective April 14, 2006.

Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.

This rule was created as part of a periodic review on January 4, 2022.

BTS-2.19 – Cloud Services Governance

Cloud Services Governance

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.19

Purpose

The information technology industry continues to shift service offerings from on-premises based systems to cloud-based services. The City of Portland is adopting cloud-based services in line with industry trends. Due care and due diligence of City information and Public Records requirements is a mandate of BTS to “ensure confidentiality, integrity and availability of electronic information...”

Administrative Rule

This policy outlines the requirements for Cloud Services use by the City of Portland and its Authorized Users per BTS-2.01. This policy applies to all City of Portland bureaus, divisions, entities and Authorized Users. Both internal City Cloud deployments (Private Cloud) and external partnerships (Public Cloud) must comply with this policy per PCC 3.15.090(B).

Cloud, or 'hosted services' take many forms, including:

IaaS – Infrastructure as a Service – The Cloud Service Provider (CSP) provides the hardware in their data center. The Cloud Consumer manages the configuration and operation of operating systems (such as Windows), databases, storage, applications, security and application use.

PaaS – Platform as a Service – The CSP provides, configures and manages the hardware, operating systems, storage and database platforms. The Cloud Consumer configures and manages the use of the platforms, application’s security and use.

SaaS – Software as a Service – The CSP provides, configures and manages the hardware, operating systems, databases, storage and applications. The Cloud Consumer manages the use of the application and may manage some aspect of application configuration and authorization of user access to the applications.

FaaS – Functions, or applications, as a Service, such as AWS (Amazon Web Services) Lambda, Kubernetes, Docker, etc.

Other - Any other cloud-based service, application, media, platform, or data repository.

Cloud Services

1. Use of Cloud Services must follow all other applicable BTS Admin rules (Technology Services | Portland.gov), City Procurement Rules (Chapter 5.33 Goods and Services | Portland.gov) and any other applicable City of Portland rules.
    a. Early engagement of BTS Information Security ensures Cloud Services align with applicable regulatory, City information security, privacy, data classification and governance requirements.
2. IaaS and PaaS
    a. For IaaS and PaaS, Bureau of Technology Services (BTS) will manage Azure, Amazon Web Services (AWS) and any other cloud provider infrastructure, platform configuration and Authorized User account access.
    b. Billing for these and other IaaS and PaaS Cloud Services will be managed through BTS. Bureaus will be responsible for monitoring and managing use of metered Cloud Services and associated costs. Billing is the responsibility of the individuals appointed as accountable for each bureau, division, or entity to monitor their data use and billing.
    c. Adjustments to Cloud Service subscriptions will be made through BTS.
3. SaaS and FaaS
    a. Use of and subscription to SaaS/FaaS must be auditable, discoverable, and capable of having information and cyber risk assessed.
    b. Cloud Services providers shall follow all applicable industry control best practices for all critical security updates and patches.
    c. SaaS/FaaS vendors must allow BTS to routinely audit their security posture or provide annual third-party auditor documentation of their security posture, which should be equivalent to a SOC 2 Type II security assessment.
    d. Cloud Services providers are expected to cooperate with City and Law Enforcement investigations of service and data availability, integrity and security, including suspected compromise or breach of data or services.
    e. Non-Standard SaaS or FaaS applications are subject to the BTS Exception Process.
4. Internal and external Cloud Services must leverage the City's Single Sign On (SSO) and Identity and Access Management (IdAM) platforms.
    a. Multi-Factor Authentication must be enabled for access to Cloud Services.
    b. Exceptions will be evaluated during the contracting process.

Legal and Contracts

1. The City's use of Cloud Services must comply with all applicable federal, state, and local laws and regulations.
    a. City Data must be always located within the United States, whether at rest, in transit, or otherwise, except as provided by BTS authorized exception.
2. All contract awards for Cloud Services must comply with City procurement code PCC 5.33 and 5.68, as applicable.
3. All contracts for Cloud Services must be submitted to the City Attorney's Office for review and approval as to form, regardless of value as required by PCC 3.10.030(B).

Data Governance, Privacy and Security

1. Bureaus managing Cloud Services data repositories must align data governance, ownership, privacy and security with City standards and requirements. (See References)

2. Bureaus must comply with City data retention policy and schedules as determined by the Auditor's Office.
    a. BTS can assist in configuring compliant IaaS and PaaS services. Also see Exit Strategy below.
3. Cloud Services containing sensitive data types are subject to additional compliance requirements, including but not limited to the following: Payment Card Industry data (PCI), Personally Identifiable Information (PII), Federal Tax Information (FTI), Criminal Justice Information Services data (CJIS), and Personal Health Information (PHI).
4. City-specific data types (Public, Restricted and Confidential) must be stored, accessed and transmitted in accordance with applicable City data governance polices, and as defined in BTS-2.18 Information Classification & Protection.

Exit Strategy

1. Cloud Services and contracts should be developed with an exit strategy for disengaging from the vendor. The City must determine how data can be recovered from the vendor and archived, if necessary, or deleted with confirmation by the vendor, at the time of contract termination or expiration.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

1. BTS Technology Definitions – https://www.portlandoregon.gov/…

2. City of Portland Security Standards
3. (BTS) Technology Standards Directory (and Acronyms) – https://www.portlandoregon.gov/…

History

Ordinance No. 179999, passed by City Council March 15, 2006, and effective April 14, 2006.

Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.

This rule was created as part of a periodic review. January 4, 2022.