



December 7, 2010

ADDENDUM #1

Re: Youth Employment Payroll Systems

Request for Proposals

PIN: 26011YEPSRFP

Dear Prospective Proposer:

Pursuant to Sections 3-02 (i) and 3-03 (f) (2) of the Procurement Policy Board Rules, the Department of Youth and Community Development (DYCD) is issuing **Addendum #1** to the **Youth Employment Payroll Systems** Request for Proposals, PIN: 26011YEPS RFP. Applicants should acknowledge receipt of Addendum #1 by using the Acknowledgement of Addenda (Attachment 6).

ADDENDUM ITEMS

- 1. Section III- Scope of Services and MWBE Requirements, page 7:** Under the heading, “Assumptions Regarding Vendor Approach,” subheading, “System Components,” a 6th bullet is added:

The system could be hosted in the City Department of Information Technology and Telecommunication (DoITT) datacenters at no cost to the vendor for hosting, bandwidth, disaster recovery, and back up services. DoITT can host on Windows, Linux and Unix.

- 2. Section III- Scope of Services and MWBE Requirements, page 7:** Under the heading, “Assumptions Regarding Vendor Approach,” subheading, “System Components,” a footnote is added to the additional 6th bullet:

¹More information regarding DoITT’s hosting offerings can be found at:
<http://www.nyc.gov/html/doitt/html/eservices/hosting.shtml>.

- 3. Section IV- Format and Content of the Proposal, page 11:** Under the heading “A2c. Proposed Approach, an additional bullet is added under “System Design:”

State whether the system can be hosted by DoITT, and, if not why.

- 4. Section IV- Format and Content of Proposal, page 12:** Under the heading “A3 Price Proposal,” the last sentence:

The Price Proposal may also include, at the option of the proposer, a price at which DYCD could, if it chose, purchase the system at the end of the term.

is deleted and replaced with the following:

The price proposal should incorporate a full-term budget including the costs of initial system development, the non-exclusive perpetual license, and modifications to the system as necessary after initial development.

- 5. Section IV- Format and Content of Proposal, page 14:** Under the heading “Proposal Package Contents (“Checklist”), subsection 3, the sentence:

A separate sealed envelope labeled “Price Proposal” containing one original set and five duplicate sets of the Price Proposal.

is deleted and replaced with the following:

A separate sealed envelope labeled “Price Proposal” containing one original set of the Price Proposal.

- 6. Section IV- Format and Content of Proposal, page 14:** Under the heading “Proposal Package Contents (“Checklist”), subsection 4, the sentence:

Price Proposal Form (Attachment 2) in a third sealed inner envelope containing:

is deleted and replaced with the following:

A third sealed inner envelope labeled “Schedule B” containing an original, completed Schedule B (see attachment 4):

- 7. A second Appendix is added:** Appendix B: DoITT Security Documents
- 8. A third Appendix is added:** Appendix C: Sample Contract Security Language
- 9. A fourth Appendix is added:** Appendix D: SYEP Application/Enrollment Data
- 10. Attachment 2: Price Proposal, pages 43-45,** is deleted and replaced with Attachment 2R

CLARIFICATIONS

- 1.** Contractors have DYCD supplied scanners (Kodak i1120 or comparable models). Scanned documents may include, but are not limited to social security cards, birth certificates, and authorization to work papers.
- 2.** Acceptable databases include MS SQL, Oracle and MYSQL. Acceptable languages include MS .NET, PHP, Ruby/RAILS. RBASE is not an acceptable database for the purposes of this RFP.

Hosting: Wintel

Description

[Service Notes](#)

[Service Levels](#)

The Wintel hosting service provides agencies with modernized, high-performance computing capacity that is ideal for compute-intensive Windows-based application workloads. DoITT offers a number of Wintel service offerings with a variety of computing capacities and service levels to address both production and preproduction hosting needs. These offerings provide agencies with an end-to-end hosting service that includes highly redundant facilities and network connectivity, physical and logical security, monitoring and reporting capabilities, and operational support. DoITT will work closely with each agency to determine the platform, capacity, and support levels that best suit the agency's needs based on the usage and performance requirements of each application.

The Wintel hosting service leverages a highly virtualized environment whenever feasible. Virtualization enables multiple application hosting environments to be hosted on a single physical machine, thereby reducing energy consumption, improving scalability, accelerating deployment of new environments, and facilitating the maintainability and recoverability of services. Whenever feasible, the default Wintel offering will be a virtual environment in order to take full advantage of these benefits. For cases in which virtualization is not feasible (e.g., load testing, highly memory-intensive requirements, compatibility constraints), dedicated environments are available.

DoITT supplies two standard Wintel offerings to meet agency requirements. For each offering, there are two standard tiers of service levels to meet the unique support requirements of agency production and preproduction environments ([visit the Service Notes section](#) for details). For all Wintel offerings, DoITT provides a variety of supporting services and capabilities ([visit the Service Notes section](#) for details).

Virtual Wintel Hosting

Virtual Wintel Hosting running Windows Servers 2008 provides agencies with highly efficient hosting solutions that are ideal for compute-intensive applications. There are four standard classes of capacity within the Virtual Wintel Hosting offering. These classes may be adjusted over time to meet changing business needs.

- Class A - 1 CPU core x 1 GB of memory
- Class B - 2 CPU core x 2 GB of memory
- Class C - 2 CPU core x 4 GB of memory
- Class D - 4 CPU core x 4 GB of memory

Dedicated Wintel Hosting

Dedicated Wintel Hosting running Windows Servers 2008 provides agencies with dedicated hosting environments when virtualization is not feasible. There are two standard classes of capacity within the Dedicated Wintel Hosting offering. These classes may be adjusted over time to meet changing business needs.

- Class A - 2 CPU core x 8 GB of memory
- Class B - 4 CPU core x 16 GB of memory

Service Notes

Custom Offerings

A custom offering may be made available as appropriate for cases where the standard offering is unable to address agency requirements; however, standard service levels described herein may not apply.

Security

DoITT makes no representation or warranty that vulnerability scans will disclose all vulnerabilities.

Division of Responsibilities

For all Wintel offerings, responsibilities are divided among the agencies and DoITT as detailed below:

DoITT supports the infrastructure and the operating system; the agency is responsible for managing and maintaining the application (unless otherwise supported by DoITT)

Application information gathering and documentation is the responsibility of the agency (unless otherwise supported by DoITT)

The agency is responsible for engaging the DoITT security liaison, agency technicians, application vendors, and others as required

All application design, programming, updates, etc., are the responsibility of the agency (unless otherwise supported by DoITT); DoITT Service Coordinators are available to facilitate requirements gathering as required

Service Levels

DoITT provides two standard service levels for all Wintel offerings:

Tier 1 service levels are provided for all virtual production environments and may be provided for dedicated production environments ([visit the Service Levels section](#) for details)

Tier 2 service levels are provided for both virtual and dedicated preproduction environments and may be provided for dedicated production environments ([visit the Service Levels section](#) for details)

Support Staff and Software Tools

All Wintel offerings include the following support staff and software tools:

Service Desk support to provide ticket-based incident, change management, and problem resolution per Information Technology Infrastructure Library (ITIL) standards

Standard reporting capabilities to provide utilization, performance, and trending information to ensure proactive identification of growth requirements (e.g., utilization tools; report generation; Syslog collection, retention, and analysis)

Capacity planning support to ensure proactive identification and active management of business demand growth (e.g., Health at a Glance)

System monitoring and management, including identification of application issues and debugging assistance to ensure high availability and application uptime (e.g., file system monitored for warning and alarm levels; security, vulnerability monitoring, and scanning)

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

All Wintel offerings include the following security support:

Security administration to provide security for data and systems (e.g., robust and secure operating environments using RACF and featuring digital certificates/public key infrastructure services, LDAP interfaces, case sensitive IDs/passwords)

Physical site security, including key cards and zoned access to different areas of the building, an on-site security force, surveillance cameras located throughout the DoITT Data Center and grounds, and a database of individuals authorized to access the facility

Technical and Engineering Support

All Wintel offerings include the following technical and engineering support:

Redundant I/O paths to support high LAN transfer rates within the datacenter; transfer rates to agency locations dependent on WAN capacities

Network tuning support to improve overall system performance and to minimize network delays

Multiple, redundant, and diverse high-speed Internet connections to supply required networking capacity and ensure connectivity

Cooling and environmental systems support to ensure primary and redundant power as required

Active load-balancing capabilities to ensure high levels of availability, reduced downtime due to maintenance and/or unforeseen incidents, and data protection

Hardware and Operating Systems Support

All Wintel offerings include the following hardware and operating systems support:

Installation and setup of all server hardware in accordance with City and industry best practices to reduce future maintenance, unplanned downtime, and engineering incidents (includes Webserver support as required)

Repair and/or replacement of hardware components under warranty shown to be detrimental to the continued operation of the system (includes Webserver support as required)

Installation, upgrades, maintenance, and monitoring support for operating systems to reduce unplanned downtime and engineering incidents

Application of firmware system patches in conjunction with the hardware operating system vendors and in accordance with City standards to ensure compliance with City policies

Application and Middleware Support

All Wintel offerings include the following application and middleware support:

Application installation and configuration to create and support application development environments as required (only applies to applications directly supported by DoITT)

Installation of security software in accordance with City and industry best practices and maintenance of antivirus software and patches to provide data and system security

Database administration support ([visit the Database Support service](#))

Data storage and backup support ([visit the Data and Storage service](#))

Data Replication, Availability Service, and Disaster Recovery support

Service Levels

Category	Metric	Assurance Level
Service Availability	Ratio of actual operating hours to	Tier 1 - 99.9%

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

	planned operating hours	Tier 2 - 99.0%
Incident Escalation	Escalation procedures for top priority incidents where a solution or workaround is expected immediately; senior management is notified as per the agreed escalation procedure	For each 20 minutes that pass without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that can operate in a degraded mode (business owner can operate in this state)	For each 2 hours that pass without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that require moderate attention where the problem may affect some users but will not have a major impact on the business	For each day that passes without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that require minimal attention where the issue is not critical and does not require immediate resolution	For each 2 days that pass without resolution, the affected agency is contacted and escalations occur
Planned Maintenance Windows	The window of time during which scheduled maintenance is performed	Contact the DoITT Agency Liaison for further details as required
Problem Management	Process incidents and problems are identified and handled	Active monitoring
Hours of Support	The window of time during which support is available to customers (subject to Availability targets)	9 am to 5 pm weekdays (best effort outside operating hours)
Virtual Provisioning Timeline	Time required to implement a new virtual hosting environment once the customer's request is completed and approved by DoITT	5 business days
Dedicated Provisioning Timeline	Time required to implement a new dedicated hosting environment once the customer's request is completed and approved by DoITT	20 business days (for standard hardware)

Hosting: Linux

Description

[Service Notes](#)

[Service Levels](#)

The Linux hosting service provides agencies with stable, high-performance computing capacity for Linux-based application workloads. DoITT offers a number of Linux service offerings across both mainframe and mid-range environments with a variety of computing capacities and service levels to address a wide range of agency hosting needs. These offerings provide agencies with an end-to-end hosting service that includes highly redundant facilities and network connectivity, physical and logical security, monitoring and reporting capabilities, and operational support. DoITT will work closely with each agency to determine the appropriate platform, capacity, and support levels to best fit the agency's needs based on the usage and performance requirements of each application.

The Linux hosting service leverages a highly virtualized environment whenever feasible. Virtualization enables multiple application hosting environments to be hosted on a single physical machine, thereby reducing energy consumption, improving scalability, accelerating deployment of new environments, and facilitating the maintainability and recoverability of services. Whenever feasible, the default Linux offering will be a virtual environment in order to take full advantage of these benefits. For cases in which virtualization is not feasible (e.g., load testing, highly memory-intensive requirements, compatibility constraints, etc.), dedicated environments are available.

DoITT supplies three standard Linux offerings to meet agency requirements. For each offering, there are two standard tiers of service levels to meet the unique support requirements of agency production and preproduction environments ([visit the Service Notes section](#) for details). For all Linux offerings, DoITT provides a variety of supporting services and capabilities ([visit the Service Notes section](#) for details).

Virtual Server Linux Hosting

Virtual Server Linux hosting running the Red Hat supported operating system provides agencies with highly efficient, low-cost hosting solutions, which are ideal for compute-intensive applications. There are three standard classes of capacity within the Virtual Server Linux offering. These classes may be adjusted over time to meet changing business needs.

Class A - 2 CPU core x 2 GB of memory

Class B - 2 CPU core x 4 GB of memory

Class C - 4 CPU core x 4 GB of memory

Dedicated Server Linux Hosting

Dedicated Server Linux hosting running the Red Hat supported operating system provides agencies with dedicated environments when virtualization is not feasible. There are two standard classes of capacity within the Dedicated Server Linux offering. These classes may be adjusted over time to meet changing business needs.

Class A - 2 CPU core x 8 GB of memory

Class B - 4 CPU core x 16 GB of memory

Mainframe z/Linux Hosting

Mainframe z/Linux hosting running the SuSe operating system provides agencies with extremely high-performance and resilient hosting solutions that are ideal for transaction-intensive workloads. The capacity for the virtual z/Linux SuSe offering will be determined based on application usage and performance requirements on a case-by-case basis and may be adjusted over time to meet changing business needs

Service Notes

Custom Offerings

A custom offering may be made available as appropriate for cases where the standard offering is unable to address agency requirements; however, standard service levels described herein may not apply.

Security

DoITT makes no representation or warranty that vulnerability scans will disclose all vulnerabilities.

Division of Responsibilities

For all Linux offerings, responsibilities are divided among the agencies and DoITT as detailed below:

- DoITT supports the infrastructure and the operating system; the agency is responsible for managing and maintaining the application (unless otherwise supported by DoITT)

- Application information gathering and documentation is the responsibility of the agency (unless otherwise supported by DoITT)

- The agency is responsible for engaging the DoITT security liaison, agency technicians, application vendors, and others as required

- All application design, programming, updates, etc., are the responsibility of the agency (unless otherwise supported by DoITT); DoITT Service Coordinators are available to facilitate requirements gathering as needed

Standard Service Levels

DoITT provides two standard service levels for all Linux offerings:

- Tier 1 service levels are provided for all virtual production environments and may be provided for dedicated production environments ([visit the Service Levels section](#) for details)

- Tier 2 service levels are provided for both virtual and dedicated preproduction environments and may be provided for dedicated production environments ([visit the Service Levels section](#) for details)

Support Staff and Software Tools

All Linux hosting offerings include the following support and software tools:

- Service Desk support to provide ticket-based incident, change management, and problem resolution per Information Technology Infrastructure Library (ITIL) standards

- Standard reporting capabilities to provide utilization, performance, and trending information to ensure proactive identification of growth requirements (e.g., utilization tools; report generation; Syslog collection, retention, and analysis)

- Capacity planning support to ensure proactive identification and active management of business

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

demand growth (e.g., Health at a Glance)

System monitoring and management, including identification of application issues and debugging assistance to ensure high availability and application uptime (e.g., File System monitored for warning and alarm levels; security, vulnerability monitoring, and scanning)

Security Support

All Linux hosting offerings include the following security support features:

Security administration to provide security for data and systems (e.g., robust and secure operating environments using RACF and featuring digital certificates/public key infrastructure services, LDAP interfaces, case sensitive IDs/passwords)

Physical site security, including key cards and zoned access to different areas of the building; an onsite security force; surveillance cameras located throughout the DoITT Data Center and grounds; and a database of individuals authorized to access the facility

Technical and Engineering Support

All Linux hosting offerings include the following technical and engineering support:

Redundant I/O paths to support high LAN transfer rates within the datacenter; transfer rates to agency locations dependent on WAN capacities

Network tuning support to improve overall system performance and to minimize network delays

Multiple, redundant, and diverse high-speed Internet connections to supply required networking capacity and ensure connectivity

Cooling and environmental systems support to ensure primary and redundant power as required

Hardware and Operating System Support

All Linux hosting offerings include the following hardware and operating system support:

Installation and setup of all server hardware in accordance with City and industry best practices to reduce future maintenance, unplanned downtime, and engineering incidents (includes Webserver support as required)

Repair and/or replacement of hardware components under warranty shown to be detrimental to the continued operation of the system (includes Webserver support as required)

Installation, upgrades, maintenance, and monitoring support for operating systems to reduce unplanned downtime and engineering incidents

Application of firmware system patches in conjunction with the hardware operating system vendors and in accordance with City standards to ensure compliance with City policies

Application and Middleware Support

All Linux hosting offerings include the following application and middleware support:

Application installation and configuration to create and support application development environments as required (only applies to applications directly supported by DoITT)

Access and support of open source packages leveraging the open source Linux platform to reduce costs

Installation of security software in accordance with City and industry best practices and maintenance of antivirus software and patches to provide data and system security

Database administration support ([visit the Database Support service](#))

Data storage and backup support ([visit the Data and Storage service](#))

Data Replication, Availability Service, and Disaster Recovery support

Service Levels

Category	Metric	Assurance Level
Service Availability	Ratio of actual operating hours to planned operating hours	Tier 1 - 99.9%
		Tier 2 - 99.0%

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

Incident Escalation	Escalation procedures for top priority incidents where a solution or workaround is expected immediately; senior management is notified as per the agreed escalation procedure	For each 20 minutes that pass without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that can operate in a degraded mode (business owner can operate in this state)	For each 2 hours that pass without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that require moderate attention where the problem may affect some users but will not have a major impact on the business	For each day that passes without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that require minimal attention where the issue is not critical and does not require immediate resolution	For each 2 days that pass without resolution, the affected agency is contacted and escalations occur
Planned Maintenance Windows	The window of time during which scheduled maintenance is performed	Contact the DoITT Agency Liaison for further details as required
Problem Management	Process incidents and problems are identified and handled	Active monitoring
Hours of Support	The window of time during which support is available to customers (subject to Availability targets)	9 am to 5 pm weekdays (best effort outside operating hours)
Virtual Provisioning Timeline	Time required to implement a new virtual hosting environment once the customer's request is completed and approved by DoITT	5 business days
Dedicated Provisioning Timeline	Time required to implement a new dedicated hosting environment once the customer's request is completed and approved by DoITT	20 business days (for standard hardware)

Hosting: UNIX

Description

[Service Notes](#)

[Service Levels](#)

The UNIX hosting service provides agencies with stable, high-performance computing capacity ideal for hosting UNIX-based applications and database instances. DoITT offers a number of UNIX service offerings with a variety of computing capacities and service levels to address both production and preproduction environments. These offerings provide agencies with an end-to-end hosting service that includes highly redundant facilities and network connectivity, physical and logical security, monitoring and reporting capabilities, and operational support. DoITT will work closely with each agency to determine the platform, capacity, and support levels that best suit the agency's needs based on the usage and performance requirements of each application.

The UNIX hosting service leverages a shared environment whenever feasible. Shared solutions enable multiple application or database hosting environments to be hosted on a single physical machine, thereby reducing energy consumption, improving scalability, accelerating deployment of new environments, and facilitating the maintainability and recoverability of services. As feasible, the default UNIX offering will be a shared environment in order to take full advantage of these benefits. For cases in which sharing is not feasible (e.g., load testing, highly memory-intensive requirements, compatibility constraints, etc.), dedicated environments are available.

DoITT supplies two standard UNIX offerings to meet agency requirements. For each offering, there are two standard tiers of service levels to meet the unique support requirements of agency production and preproduction environments ([visit the Service Notes section](#) for details). For all UNIX offerings, DoITT provides a variety of supporting services and capabilities ([visit the Service Notes section](#) for details).

Shared UNIX Hosting

Shared UNIX hosting provides agencies with a highly efficient solution for hosted UNIX applications, which scales easily, accelerates the deployment of new environments, and facilitates the maintainability and recoverability of services.

The Shared UNIX hosting standard offering for application hosting is Sun Solaris 10 on SPARC. There are four standard classes of capacity within the Shared SPARC offering. These classes may be adjusted over time to meet changing business needs.

Class A - 4 threads x 2 GB of memory

Class B - 4 threads x 4 GB of memory

Class C - 8 threads x 4 GB of memory

Class D - 8 threads x 8 GB of memory

The Shared UNIX hosting standard offering for database hosting is Sun Solaris 10 on x86. There are three standard classes of capacity within the Shared x86 offering. These classes may be adjusted over time to meet changing business needs.

Class A - 1 CPU core x 4 GB of memory

Class B - 2 CPU core x 8 GB of memory

Class B - 4 CPU core x 16 GB of memory

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

Dedicated UNIX Hosting

Dedicated UNIX hosting provides agencies with a highly efficient dedicated hosting solution when a shared hosting environment is not feasible.

The Dedicated UNIX hosting standard offering for application hosting is Sun Solaris 10 for SPARC. There is a standard class of capacity within the Dedicated SPARC offering. This class may be adjusted over time to meet changing business needs.

Class A - 64 threads x 32 GB of memory

The Dedicated UNIX hosting standard offering for database hosting is Sun Solaris 10 for x86. There are two standard classes of capacity within the Dedicated x86 offering. These classes may be adjusted over time to meet changing business needs.

Class A - 2 CPU core x 8 GB of memory

Class A - 4 CPU core x 16 GB of memory

Service Notes

Custom Offerings

A custom offering may be made available as appropriate for cases where the standard offering is unable to address agency requirements; however, standard service levels described herein may not apply.

Security

DoITT makes no representation or warranty that vulnerability scans will disclose all vulnerabilities.

Division of Responsibilities

For all UNIX offerings, responsibilities are divided among the agencies and DoITT as detailed below:

DoITT supports the infrastructure and the operating system; the agency is responsible for managing and maintaining the application (unless otherwise supported by DoITT)

Application information gathering and documentation is the responsibility of the agency (unless otherwise supported by DoITT)

The agency is responsible for engaging the DoITT security liaison, agency technicians, application vendors, and others as required

All application design, programming, updates, etc., are the responsibility of the agency (unless otherwise supported by DoITT); DoITT Service Coordinators are available to facilitate requirements gathering as needed

Service Levels

DoITT provides two standard service levels for all UNIX offerings:

Tier 1 service levels are provided for all shared production environments and may be provided for dedicated production environments ([visit the Service Levels section](#) for details)

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

Tier 2 service levels are provided for both shared and dedicated preproduction environments and may be provided for dedicated production environments ([visit the Service Levels section](#) for details)

Support Staff and Software Tools

All UNIX offerings include the following support staff and software tools:

Service Desk support to provide ticket-based incident, change management, and problem resolution per Information Technology Infrastructure Library (ITIL) standards

Standard reporting capabilities to provide utilization, performance, and trending information to ensure proactive identification of growth requirements (e.g., utilization tools; report generation; Syslog collection, retention, and analysis)

Capacity planning support to ensure proactive identification and active management of business demand growth (e.g., Health at a Glance)

System monitoring and management, including identification of application issues and debugging assistance to ensure high availability and application uptime (e.g., File System monitored for warning and alarm levels; security, vulnerability monitoring, and scanning)

Security Support

All UNIX offerings include the following security support:

Security administration to provide security for data and systems (e.g., robust and secure operating environments using RACF and featuring digital certificates/public key infrastructure services, LDAP interfaces, case sensitive IDs/passwords)

Physical site security including key cards and zoned access to different areas of the building, an onsite security force, surveillance cameras located throughout the DoITT Data Center and grounds, and a database of individuals authorized to access the facility

Technical and Engineering Support

All UNIX offerings include the following technical and engineering support:

Redundant I/O paths to support high LAN transfer rates within the datacenter; transfer rates to agency locations dependent on WAN capacities

Operating system kernel and network tuning support to improve overall system performance and to minimize network delays

Multiple, redundant, and diverse high-speed Internet connections to supply required networking capacity and ensure connectivity

Cooling and environmental systems support to ensure primary and redundant power as required

Hardware and Operating System Support

All UNIX offerings include the following hardware and operating system support:

Installation and setup of all server hardware in accordance with City and industry best practices to reduce future maintenance, unplanned downtime, and engineering incidents

Repair and/or replacement of hardware components under warranty shown to be detrimental to the continued operation of the system

Installation, upgrades, maintenance, and monitoring support for operating systems to reduce unplanned downtime and engineering incidents

Application of firmware system patches in conjunction with the hardware operating system vendors and in accordance with City standards to ensure compliance with City policies

Application and Middleware Support

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

All UNIX offerings include the following application and middleware support:

Application installation and configuration to create and support application development environments as required (only applies to applications directly supported by DoITT)

Installation of security software in accordance with City and industry best practices and maintenance of antivirus software and patches to provide data and system security

Database administration support ([visit the Database Support service](#))

Data storage and backup support ([visit the Data and Storage service](#))

Data Replication, Availability Service, and Disaster Recovery support

Service Levels

Category	Metric	Assurance Level
Service Availability	Ratio of actual operating hours to planned operating hours	Tier 1 - 99.9%
		Tier 2 - 99.0%
Incident Escalation	Escalation procedures for top priority incidents where a solution or workaround is expected immediately; senior management is notified as per the agreed escalation procedure	For each 20 minutes that pass without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that can operate in a degraded mode (business owner can operate in this state)	For each 2 hours that pass without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that require moderate attention where the problem may affect some users but will not have a major impact on the business	For each day that passes without resolution, the affected agency is contacted and escalations occur
	Escalation procedures for production systems that require minimal attention where the issue is not critical and does not require immediate resolution	For each 2 days that pass without resolution, the affected agency is contacted and escalations occur
Planned Maintenance Windows	The window of time during which scheduled maintenance is performed	Contact the DoITT Agency Liaison for further details as required
Problem Management	Process incidents and problems are identified and handled	Active monitoring
Hours of Support	The window of time during which support is available to customers (subject to Availability targets)	9 am to 5 pm weekdays (best effort outside operating hours)
Shared Provisioning Timeline	Time required to implement a new shared hosting environment once the customer's request is completed and approved by DoITT	5 business days
Dedicated Provisioning	Time required to implement a new dedicated hosting environment once	20 business days (for standard hardware)

APPENDIX B: DoITT Security Documents

Youth Employment Payroll Systems RFP

PIN: 26011YEPSRFP

Timeline	the customer's request is completed and approved by DoITT	
-----------------	---	--



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

IDENTITY MANAGEMENT

THE POLICY

ALL ACCESS TO CITY OF NEW YORK SYSTEMS MUST BE AUTHORIZED AND BASED UPON INDIVIDUAL IDENTIFICATION AND AUTHENTICATION.

AGENCY RESPONSIBILITY

- 1) Each agency is responsible for the management of its user identities. This includes identity validation/registration, authentication, authorization, provisioning/de-provisioning and management of identities.
- 2) Management approval is required before a user is authorized to use any City computing resources.
- 3) Users who are not City employees, but who are in a current contractual relationship with the City may have access to City computing resources if they have a valid non-disclosure agreement in effect and their sponsor approves their access.

IDENTITY LIFE CYCLE

- 4) Users must be positively and individually identified and validated prior to being permitted access to any City computing resource.
- 5) Users will be authenticated at a level commensurate to the data classification of the information being accessed.
- 6) Access permissions must be defined in accordance with a user's actual functional work requirements.
- 7) User accounts will be created and de-provisioned in a timely manner. Inactive user accounts will be de-provisioned according to the **Citywide Information Security Password Policy**.

CITYWIDE IDENTITY STORE

- 8) Each agency must establish connectivity to the DoITT managed Enterprise Directory.
- 9) Each agency is responsible for managing their identities within the DoITT managed Enterprise Directory/Identity Vault.
- 10) All applications used by multiple agencies or which support external users are required to utilize the DoITT managed Enterprise Directory for authentication.
- 11) Applications will be required to participate in the consolidation of external identities to the DoITT managed Enterprise Directory.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

PASSWORD CONTROLS

- 12) The password settings of user accounts must comply with the ***Citywide Information Security Password Policy***.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Identity Management Standard

Objective

This standard provides the identity management configuration requirements which agencies connected to the DoITT-managed Enterprise Directory, NYC.ID, must follow. Consistent adherence to these requirements facilitates the ongoing accuracy, manageability and security of the Citywide enterprise directory.

Audience and Scope

This standard applies to all City of New York agencies/employees and to consultants, vendors and other organizations that are authorized to perform account administration on any identity management system connected to the DoITT managed Enterprise Directory.

The scope of this standard includes all identity management systems connected to NYC.ID.

Background

The Citywide Enterprise Directory, NYC.ID, connects to most agency directories providing account authentication and authorization for Citywide applications such as Siebel Analytics and PMA. It also provides password self-service, support for desktop single sign-on and automated account de-provisioning.

Agency Container Requirements

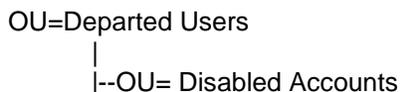
- 1) The connectors to the internal NYC.ID system are for all internal users, including consultants, contractors and interns. This is required for Citywide application access as well as for whitepages services as part of inter-agency interactions.
- 2) Service accounts used exclusively by automated processes (not used by people) must not synchronize to the NYC.ID. They must be kept in separate containers (OUs) which are excluded from synchronization.
- 3) Separate containers (OUs) must be used for employee and non-employee accounts. At the account level, "EmployeeType" must be used to differentiate employee and non-employee accounts. For agencies supported by NYCAPS, please see the "Data Formatting Requirements" section later in this document related to population of EmployeeID information as well as EmployeeType requirements.
- 4) Generic accounts are not permitted. If they exist and cannot be eliminated immediately they must be placed in containers that are excluded from synchronizing to NYC.ID.
- 5) Each agency must create and use a "CityWideGroups" container for groups which are synchronized to the NYC.ID environment. The only groups in this container should be those required for Citywide applications and for NYC.ID services such as role management for Citywide applications.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Agency Account De-provisioning Requirements

- 6) Agencies must follow a two-step account de-provisioning process using a “Departed Users” container and a subordinate container called “Disabled Accounts” as follows:



This table shows the results of moving accounts in and out of these containers.

Change made in Agency directory	Resulting action in CityWide directory
Account is moved into <i>Departed Users</i> container.	User account is disabled in NYC.ID. If account was erroneously moved, this change can be reversed with no issues.
Account is moved into <i>Disabled Accounts</i> container.	User account is removed from NYC.ID. All Citywide application group memberships and password synchronization are lost.
Account is moved out of <i>Departed Users</i> container (into synchronized container).	<i>Login disabled</i> setting is synchronized from setting in Agency directory.

The connector to the Citywide Directory must be updated to support these settings (if this has not already been done at agency.)

- 7) Automated account de-provisioning for NYCAPS agencies will become a mandatory configuration in the future as part of NYC.ID Citywide automated provisioning and role management.
- 8) Account names and Email addresses must not be re-used upon de-provisioning. This is to prevent issues with the NYC.ID services, integrated data sources and applications that need to store user profiles with historical information tied to account names (for example Document Management systems).
- 9) Upon permanent disabling of accounts, all group memberships and other rights (such as file share access) must be updated to remove the account from access in order to ensure that only active users are listed when reviewing rights.

Application Requirements

- 10) Applications integrated with NYC.ID (Citywide applications) must:
- a. Not store user credentials that are used to authenticate to the NYC.ID services.
 - b. Handle their own application specific user profile management needs including synchronization management.
 - c. Handle their own cleanup of application user profiles.
 - d. Use available NYC.ID services for external account registration and authentication for public facing applications.
 - e. Use available NYC.ID Business Partner/Known User services to manage any non-CityNet users requiring access to an internal CityNet application. This is



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

combined with the DoITT SSL/VPN services to enable password management and application access. (This eliminates the problematic historical use of agency LAN accounts for non-CityNet users which complicated the identity and password management process. Please refer to the NYC.ID documents on integrating internal applications or contact the NYC.ID team for further details.)

Other Requirements

- 11) All non-employee accounts (both onsite and offsite) must be reviewed periodically by the authorizing employee/manager to ensure access rights are still appropriate and the account is still needed.
- 12) Agency must not add user accounts from other agencies to its directory or applications. Doing so causes discrepancies in the Citywide enterprise directory such as duplicate email IDs. Applications serving multiple agencies are considered Citywide applications and must adhere to the Citywide Identity Management Policy which requires them to integrate with NYC.ID.
- 13) Agency directories must not use personal/external email addresses for internal accounts. Agency use of external email addresses can bypass email archiving/discovery processes and expose information sent via Internet based email, leaving the agency unable to investigate potential regulatory, legal and business issues.
- 14) Agency managed accounts must be configured to comply fully with the Citywide Password Policy (e.g., password complexity, age, history, expiration and lockout).
- 15) Agency must document existing email domain names used and inform the DoITT NYC.ID team when new domains are required.
- 16) Agency must maintain accurate and up-to-date account contact information.
- 17) All agencies/units supported by NYCAPS, must ensure a dynamic bi-directional supported connector is implemented to enable application/service delivery, automated provisioning/de-provisioning and application role management.
- 18) The NYC.ID infrastructure supports connectors for authoritative data sources for the core user identity (for example Peoplesoft for EmployeeID, Pinnacle for work telephone number, and primary agency directory for email address and password). NYC.ID also supports connectors where the NYC.ID infrastructure cannot be utilized for authentication and authorization (for example z/OS or RACF).

All other applications must use LDAP query mechanisms for obtaining core user identity information for updating user profile information within their databases. Applications can use vendor import processes, custom LDAP scripts/tools, or integration products such as Directory Wizards, SimpleSync, Tivoli Directory Integrator (TDI), Oracle Data Integrator, various LDAP client tool/scripts or API interfaces to update user profile information into an application database.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Data formatting requirements:

- 19) The EmployeeID attribute must be the 7 digit number from NYCAPS/PMS, including leading zeros. Example: 0123456, 0012345, or 1234567. Any non-NYCAPS/PMS numbers must be stored in a different attribute than the one used for NYCAPS/PMS numbers.
- 20) For all NYCAPS agencies – the NYCAPS/PMS Employee ID must be stored in the EmployeeID attribute for each user account in the agency's LAN environment.
- 21) The EmployeeID attribute must be synchronized bi-directionally to the Citywide Directory for purposes of Citywide Identity Management efforts – including reporting and automated de-provisioning.
- 22) Non-employees should be assigned an ID of the form "C" + 3-digit Agency Code (or Business Unit if applicable) + a 6-digit number managed by the agency (example: C858123456).
- 23) EmployeeType attribute must be set as follows for all NYCAPS agencies:
 - Use 'E' for all NYCAPS registered employees and interns
 - Use 'C' for consultants/contractors/vendors
 - Use 'I' for interns that are not paid from NYCAPS/PMS.
 - Use 'B' for business partners.
 - Use 'T' for test accounts.
 - Use 'S' for service accounts.
- 24) Telephone Numbers must be formatted as follows:
 - (xxx) yyy-zzzz or (212) 555-1212
 - An optional space delimited extension may be added if applicable as follows:
(xxx) yyy-zzzz xzzz or (212) 555-1212 x123
- 25) Whitespace and special characters may not be used in the account name. If account name is used as part of the Email address, the limitations described in the Internet RFC 5322 and RFC 5321 standards also apply.
- 26) The last name field for each account must be populated in the agency directory in order for synchronization to NYC.ID to occur.
- 27) Email addresses must meet RFC 5322 and RFC 5321 requirements.

Definitions

- 28) Authoritative Data Source – an application or database providing the "master" source of core account information on a user in the NYC.ID infrastructure.
- 29) Provisioning – The process of automating the creation/deletion of accounts used for authentication, authorization and storing authoritative data required by NYC.ID. Provisioning also includes the processes required to activate assets/services for a user via the Citywide Remedy ARS platform, necessary to provide users with resources/assets/services and associate the assets/services with the user.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 30) Identity Connector – technology used to synchronize the core user identity information to/from authoritative data sources.
- 31) External User – a public user/citizen accessing internet facing applications. This can include any “self-registration” customer such as small businesses as well.
- 32) Business Partner/Known User – a user outside CityNet requiring access to an internal CityNet application. These users are sponsored by the City Agency/Application Owner.
- 33) Agency – an agency/organization authorized for access to CityNet – typically restricted to NYCAPS registered organizations.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Password Policy

The Policy

All passwords and Personal Identification Numbers (PINs) used to protect City of New York systems must be appropriately configured, periodically changed, and issued for individual use.

Password/PIN Usage and Confidentiality

- 1) Individual users must properly protect passwords and/or PINs for all accounts.
- 2) All passwords and/or PINs must be classified and handled as City of New York PRIVATE data.
- 3) Passwords and/or PINs unique to an individual must not be shared with other individuals or users.
- 4) Passwords/PINs must not be displayed on the screen at any time.
- 5) Passwords and/or PINs must be changed whenever there is any indication of system or password compromise.
- 6) Any password or PIN management system either must avoid caching the password or PIN or must provide adequate protections and controls if such caching is essential.
- 7) Passwords and/or PINs must always be encrypted when held in storage or when transmitted across any network. Exception: One-time passwords or PINs, or hard-coded passwords or PINs
- 8) Use of a City of New York approved hashing algorithm is considered encryption for the purposes of password or PIN protection. Unencrypted passwords and/or PINs must never be embedded in sign-on utilities. For example, an unauthorized user must never be able to authenticate at sign-on merely by using a function key or by running an available program.
- 9) Unencrypted passwords and/or PINs must not be hard-coded in source code, command files, initialization files, scripts or installation kits.
- 10) PINs shall only be used where a numeric method for authentication is required (e.g., for entry on a telephone keypad); in all other instances, passwords should be used for authentication.
- 11) Administrative passwords must be adequately protected and restricted only to required individuals for system support.
- 12) Screen lock must be activated within fifteen (15) minutes of unattended inactivity.

Password/PIN Length

- 13) Passwords and/or PINs must have a minimum length of eight (8) characters. Exception: Voice mail systems, as well as Blackberry and PDA devices issued by the City must use a password or PIN of at least 4 alphanumeric characters.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Password Complexity

- 14) Passwords must be constructed using at least one alphabetic and at least one character which is numeric or a special character.

Class Description	Examples
1. Upper Case Letters	A B C ... Z
2. Lower Case	a b c ... z
3. Numerals	0 1 2 ... 9
4. Non-alphanumeric ("special characters", punctuation, symbols)	{ } [] , . < > ; : ' " ? / \ ` ~ ! @ # \$ % ^ & * () _ - + =

- 15) Passwords must not be derived from commonly used words or phrases.
- 16) Users should not select passwords consisting of easily guessed words, such as words found in dictionaries (English and non-English), User IDs, proper names or other names or words readily associated with the individual user, such as dates, nicknames and family names.
- 17) Users should not select passwords, or PINs, that contain personally identifiable numbers, such as the user's telephone extension, Social Security Number, or zip code.

Password/PIN Expiration

- 18) Passwords and/or PINs must be changed at least every ninety (90) days.
- 19) Temporary or initial passwords and/or PINs must be set to expire after initial use. The user must be required to change the password or PIN at the first use.
- 20) Administrative passwords must be changed every sixty (60) days, or when an individual who has knowledge of the password leaves their job function.

Disabling of Accounts

- 21) All accounts that provide access to SENSITIVE, PRIVATE or CONFIDENTIAL Information must be automatically disabled after five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

Default Passwords/PINs

- 22) Any default password or PIN must be changed during or immediately upon the completion of the installation process. The new password or PIN must conform to the requirements defined in this policy.
- 23) Default accounts must be renamed, if possible, to non-obvious names.

Password/PIN Reuse

- 24) User-chosen passwords and/or PINs must not be reused for four (4) iterations.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Password/PIN Changes

- 25) Proper proof of identification must be provided before changing a password or PIN.
- 26) Users changing a password or PIN via a system command or screen must prove knowledge of the current password or PIN or be cryptographically authenticated before being allowed to change it.
- 27) The minimum time between user initiated password and/or PIN changes must be at least one (1) day. If a user has recently changed a password and is concerned that the new password may have been compromised, but is unable to immediately change it again in accordance with this provision, the user should contact an administrator of the system in which the password is used to request a password reset.
- 28) Users requesting a new password or PIN or requesting a password or PIN change/reset via a help desk or administrator must prove their identity before the change is initiated.

Password/PIN Delivery

- 29) Delivery of passwords and PINs to a user, either when an account is created or when an administrator resets a password/PIN, requires attention to ensure that delivery is done efficiently and with a regard to security. Passwords must not be transmitted over any City of New York voice, video or data network without appropriate identification and authentication.
- 30) A password must be delivered in a manner that requires the recipient to prove his/her identity before the password is received.

Policy Enforcement

- 31) Administrators are accountable for configuring systems to enforce this policy.
- 32) Where possible, the system must enforce these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures. For example, to enforce password complexity, the administrator should run tools periodically to detect weak passwords, and require users with weak passwords to change their passwords.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Data Classification Policy

The Policy

The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background

To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope

This policy applies to all information. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

Information Classification

All information at the City of New York and corresponding agencies will be classified at one of four levels; Public, Sensitive, Private, or Confidential.

- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency's ability to perform its primary business function.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Information Valuation and Categorization

- 1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
- 2) All information assets must be valued and categorized.
- 3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
- 4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Data Steward

- 5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- 6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.
- 7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.
- 8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.

Information Labeling

- 9) Information within systems or processes must be marked appropriately to ensure that users will be aware of the sensitivity of the information and how it should be protected and controlled. Appropriate marking of mission critical information includes marking it as Public, Sensitive, Private, or Confidential.
- 10) All copies or reproductions maintain the same level of classification as the original.
- 11) Aggregation of data with different classification levels require reevaluation to determine if a new level of classification is needed.
- 12) All personally identifiable information should be classified at a minimum as Private.

Information Protection

- 13) Protective measures must take into account the value associated with unauthorized access or loss of information assets.
- 14) Data classified as Private or Confidential must be protected and secured during any electronic data transmission or electronic or physical media transfer.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 15)** Data classified as Private or Confidential may not be transmitted electronically over Citynet¹ without encryption.
- 16)** Data classified as Private or Confidential may not be transmitted over a public network (such as the Internet) unless it is in an approved, encrypted form.

¹Metro area network utilized by multiple agencies and supported by DoITT
Issued: July 28, 2008 Final Version 1.2



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

DATA CLASSIFICATION STANDARD

OBJECTIVES

In support of the Data Classification Policy, this standard defines an assessment methodology for determining the data classification of a data-set.

AUDIENCE AND SCOPE

This standard applies to all organizations, individuals, employees, vendors and contractors that work with City of New York data.

Directly affected functions consist of:

- Business owners
- Data custodians
- Project Managers
- Information Security Managers
- Application Developers
- Application/system owner

Background

To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

DATA CLASSIFICATION OVERVIEW

Data is classified by analyzing the risk to the agency and City of New York in the event of unauthorized disclosure, modification or deletion of data. Risk includes financial (law suits, grant loss, user notification/credit monitoring costs), loss of reputation and good will, negative political exposure to public figures, and safety and well being of the public.

There are specific laws and regulations that govern certain kinds of data such as the NYC Administrative Code, NYS Breach Notification Law, HIPPA, FERPA, and Gramm-Leach-Bliley. If data is determined to be PII (Personally Identifiable Information) or PHI (Personal Health Information) by any legislation, it automatically becomes classified as PRIVATE.

Contextual analysis plays an important role in any data classification decision. As an example, the following dataset could be classified at SENSITIVE: {First Name and Last Name}. However, if it can be determined that this dataset originated from a list of medical patients with a particular medical condition, it would fall under the category of PHI and needs to be classified as PRIVATE.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

PII (Private Identifiable Information)

The following elements are examples of PII, as defined by Federal, State, and Local legislation:

1. Date of birth
2. Social security number
3. Driver’s license number
4. Non-driver photo identification card number
5. Any Financial services account number or code (credit card, checking, savings brokerage account, ATM number, etc)
6. Personal identification number
7. Mother’s maiden name
8. Computer system password
9. Electronic signature
10. Unique biometric data that is a fingerprint, voice print, retinal image or iris image

PHI (Private Health Information)

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

DATA CLASSIFICATION CATEGORIES

Data Classified as PUBLIC

Datasets that are purposefully made available through mass distribution channels (web sites or open publication) could be classified as PUBLIC. This data has no requirement for confidentiality. However, controls have to be in place to prevent unauthorized modification of the data (integrity) and to ensure continued access to the data (availability).

Examples of How Data Integrity and Availability can be affected	Impact
<ul style="list-style-type: none"> • A Web Site (such as www.nyc.gov) is compromised and information is modified. 	Public is served with misleading and incorrect information which could lead to loss.



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

<ul style="list-style-type: none">• A Web Site (such as www.nyc.gov) is compromised and is prevented from presenting the information or information is deleted.	Public is prevented from viewing the information which could lead to loss.
--	--

Data Classified as SENSITIVE

Datasets that are not classified as PRIVATE (see below), yet are not made publically available through mass distribution channels (web sites or open publications) is classified as SENSITIVE. This category includes information subject to Freedom of Information Law inquiries. This data has some requirements for confidentiality and controls have to be in place to prevent unauthorized modification of the data (integrity) and to ensure continued access to the data (availability).

Data Loss	Impact
<ul style="list-style-type: none">• A list of email addresses signed up for mail distribution is released.	This list can now be used in sending SPAM to the users and will cause a nuisance condition which will be attributed to the City.
<ul style="list-style-type: none">• Name, address, and phone number of a person making a noise complaint is released.	This information disclosure could have a negative effect on how the public trusts the City.

Data Classified as PRIVATE

Datasets containing PII or PHI, are protected by legislation, or that is deemed too important to be published via channels normally used for PUBLIC or SENSITIVE information automatically classified at PRIVATE. This data has strict requirements for confidentiality and controls have to be in place to prevent unauthorized modification of the data (integrity) to ensure continued access to the data (availability).



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Data Loss	Impact
<ul style="list-style-type: none"> • A list of names and social security numbers is stolen from a financial system database. • Health records are compromised. • An Employee maliciously accesses personal records of taxpayers and sells them to criminals. 	<ul style="list-style-type: none"> • Individuals are exposed to potential identity theft. • Long term loss of reputation. • Public official has to apologize for data loss. • Payment for credit monitoring services.

Data Classified as CONFIDENTIAL

Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is automatically classified at CONFIDENTIAL.

Data Loss	Impact
<ul style="list-style-type: none"> • A list of names of undercover law enforcement officers is sold to criminals. • Disclosure of a dignitary protection plan • Loss of control of a SCADA system. 	<ul style="list-style-type: none"> • Obstruction of a criminal investigation • Long term loss of reputation. • Danger to public safety • Loss of life

NOTE: CityNet is not designed to store, transmit or host systems that transact confidential data.

Data Classification Matrix

If data does not clearly fall into one of the 4 data classification levels, you can use a CIA (Confidentiality, Integrity and Availability) matrix to identify data classifications.

- **Confidentiality:** The need to strictly limit access to data to protect it from loss.
- **Integrity:** Data must be accurate, and users must be able to trust its accuracy.



**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

- **Availability:** Data must be accessible to authorized persons, entities, or devices.

Select the most important element in the dataset and apply the following decision matrices:

Data Classification			
	PRIVATE	SENSITIVE	PUBLIC
Need for Confidentiality	Required	Recommended	None
	AND/OR	AND/OR	AND/OR
Need for Integrity	Required	Required	Recommended
	AND/OR	AND/OR	AND/OR
Need for Availability	Required	Required	Required

Data Classification	Unauthorized Disclosure	Loss of Data Integrity	Access to the Data is Denied
PUBLIC	None	Damage to the reputation of the City	Damage to the reputation of the City
SENSITIVE	Management censure	City management decision making process is compromised	City management decision making process is compromised
PRIVATE	<ul style="list-style-type: none"> • Severe financial and reputation loss to the City • Legal action 	City management decision making process is severely compromised	City management decision making process is severely compromised
CONFIDENTIAL	<ul style="list-style-type: none"> • Severe financial and reputation loss to the City • Threat to life safety • Criminal legal action 	Threat to life safety	Threat to life safety



**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

REFERENCES:

NYC Administrative Code, Title 10, Chapter 5,

§ 10-501 Definitions. For the purposes of this chapter,

a. The term "personal identifying information" shall mean any person's date of birth, social security number, driver's license number, non-driver photo identification card number, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person. This term shall apply to all such data, notwithstanding the method by which such information is maintained.

New York State General Business Law,

§ 899-aa. Notification; person without valid authorization has acquired private information. 1. As used in this section, the following terms shall have the following meanings:

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; or

(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

New York State Technology Law

§ 208. Notification; person without valid authorization has acquired private information. 1. As used in this section, the following terms shall have the following meanings:

(a) "Private information" shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- (1) social security number;
 - (2) driver's license number or non-driver identification card number;
- or
- (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

- (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- (2) indications that the information has been downloaded or copied; or
- (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(c) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

- (1) the judiciary; and
- (2) all cities, counties, municipalities, villages, towns, and other local agencies.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of cyber security and critical infrastructure coordination to determine the scope of the breach and restoration measures.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and

(3) notification to major statewide media.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer



**THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS**

reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

NIST Publication SP800-122 “*Guide to Protecting the Confidentiality of Personally Identifiable Information*”

“Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.”

HIPPA

"(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that--

"(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

"(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and--

"(i) identifies the individual; or

"(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Guideline for Security Language in Contracts

Consultant and Consultant Organizational Responsibility

1. The vendor is responsible for the adherence, by Vendor provided resources, to all Citywide Information Security Policies and Standards as published by DoITT.
2. Vendor shall surface issues, suggest options, and make recommendations to the City with regard to security, based upon the classification of application data as described in the City's Data Classification Policy.
3. All staff and consulting resources provided by the Vendor are required to acknowledge receipt of the Citywide User Responsibilities Policy
4. Vendor will be required to adhere to Citywide policies, standards, and best practices for information security, application and systems network architecture, disaster recovery, and the secure storage and transmission of data.

High-level Policy Requirements are as follows:

1. Citynet Architecture Standard – all systems must meet the requirements as defined.
2. Anti Virus – appropriate use to prevent the introduction of viruses and other forms of malicious code into the network environment
3. Change Control – structured process to encapsulate, schedule and implement any changes that impact the production environment
4. Copyright Compliance – ensure compliance with the terms of all software licenses utilized in the system
5. Data Classification – all data classified and appropriate controls utilized in accordance with the sensitivity of the data
6. Encryption – encrypting the data to ensure privacy and confidentiality
7. Password Management – appropriate password controls including complexity requirements, masking when entering, and auto expiration
8. Remote Access – third party technical support accounts must be removed or disabled after the required activities are completed. Auditing must be enabled on all vendor and third party user accounts.
9. Vulnerability Management – Systems must be monitored for vulnerabilities.
10. Security Accreditation – all multi-agency and Internet facing systems must meet the requirements of Accreditation Process
11. Other policies and standards published publically on NYC.gov and privately on Cityshare

Additional Requirements

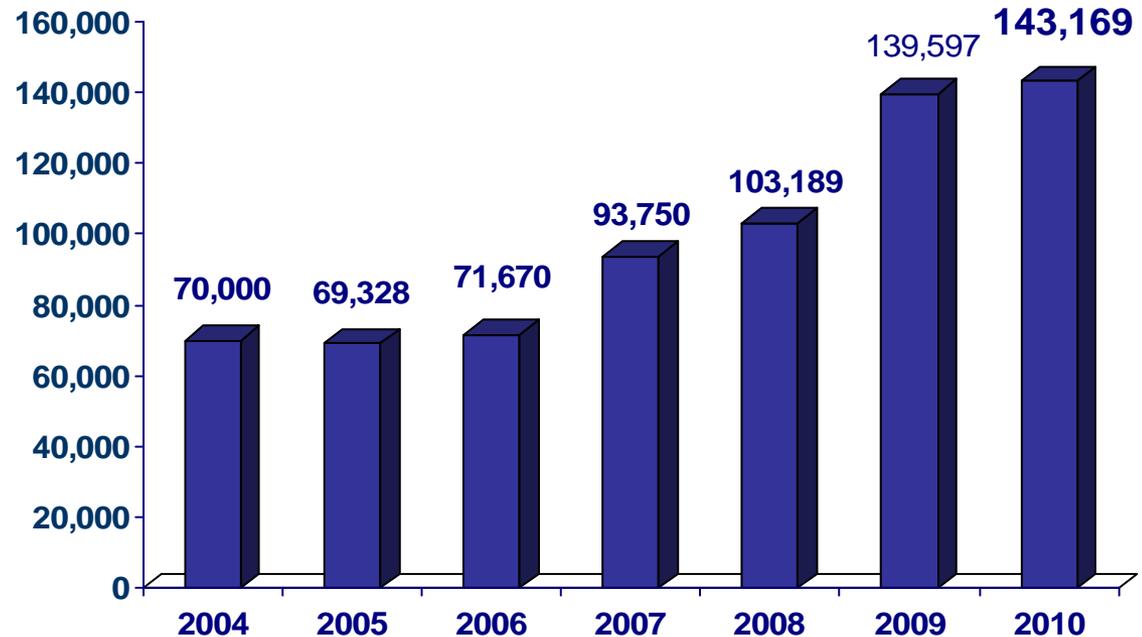
1. System auditing – integration with existing monitoring systems, and internal capabilities to generate audit logs.

2. Records retention capabilities that meet Citywide standards, including *13:45F-3.5 Destruction of certain records*
3. Privacy and Handling of Private Information – The protection of the privacy of personal information is of utmost importance. Privacy of an individual's information must be respected and maintained throughout its lifetime. Data may only be used for its intended purpose and may not be shared.
4. Personnel Security Policy – vendors assigned to City projects must conduct adequate background checks for each consultant assigned in order to reduce the risks of human error, theft, or misuse of the City's information assets
5. Non-disclosure agreements – Vendors and their contractors will be required to sign non-disclosure agreements acknowledging their responsibilities to maintain the confidentiality of City of New York information, compliance to Citywide Information Security policies, and agreement to report violations

Applications

- **143,169 applications received in 2010**
- **Over 80% submitted online**

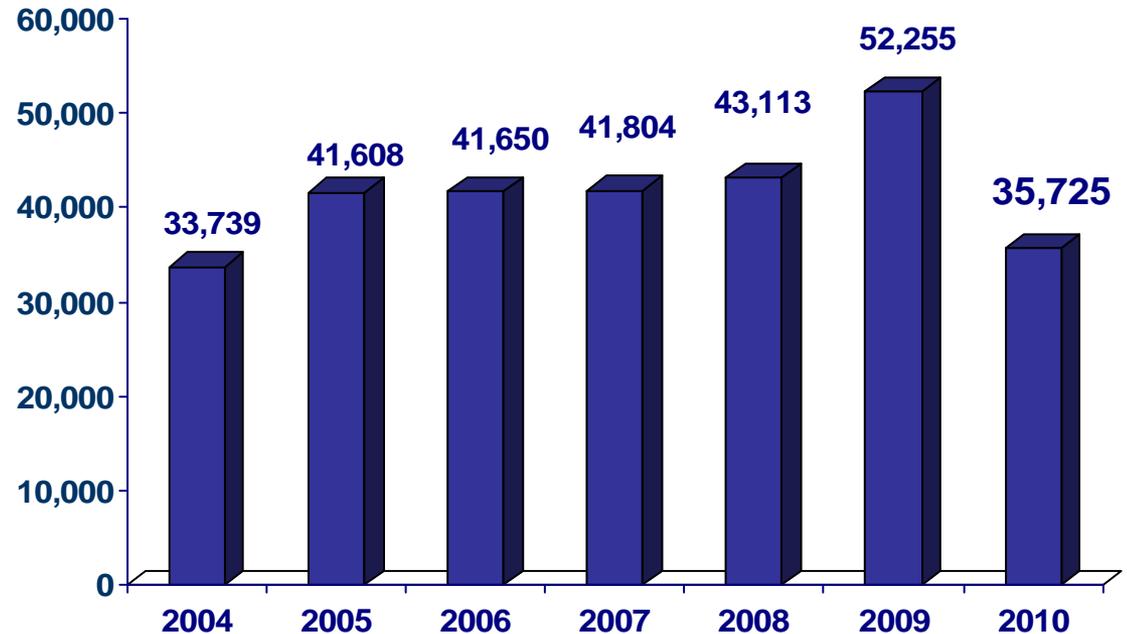
Applications Received



Enrollment

- 35,725 participants enrolled in 2010
- 25% of applicants accepted

Participants Enrolled



**For categories on this page, Price is based on 30,000 participants.
Additional quantity amounts = 10,000.**

	Price	Price for Additional Quantities
D. Banking Processes		
1. Transactions fees with Bank [loading debit cards, etc.]	\$	\$
2. Debit Cards [fees for use of card, etc.]	\$	\$
3. Fees for distribution/mailing of Debit Cards [including any costs for replacement of lost/damaged Debit Cards]	\$	\$
4. Data Reporting from Bank	\$	\$
Total Price for Banking Processes	\$	\$
E. W-2s		
1. Production, distribution, mail returns [loading debit cards, postage, etc.]	\$	\$
Total Price for W-2s	\$	\$
F. Help Desk		
DYCD Contractors	\$	
Program Participants	\$	\$
Total Price for Help Desk	\$	\$
G. Training		
Initial system training	\$	
Program Model A - Yearly user (contractor) training	\$	
Program Model B – Periodic user (contractor) training	\$	
System upgrades training	\$	
Total Price for Training	\$	
H. System Modifications		
Cost for general modifications to the system by quantity (50 or 100 hours)	\$	
Total Price for System Modifications	\$	

Pricing for Additional Programs/Services

I. Additional Programs/Services

Incremental cost for inclusion of a new program (as identified on page 7, subsection B. of this RFP.) to the overall system.

Total Price for Additional Programs/Services

\$	
\$	