Information Technology Board Meeting

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Information Technology Board Meeting: Agenda

Meeting Details:

Date: November 19, 2024 **Time:** 9:30 AM

Location: City County Building, Room 260

Chairman: Joseph O'Connor **CIO:** Collin Hill

Roll Call:

1. **Chairman O'Connor**

IT Board Business:

2. **Approval of the October 29, 2024, Meeting Minutes**: Chairman O'Connor

Status Updates:

3. **ISA Board Report**: Collin Hill, CIO, ISA
4. **ISA Financial Report:** Kai Davis, CFO, ISA

Action Items:

5. **Resolution 24-63: Flock Group, Inc. –** Deputy Chief Kevin Wethington, Indianapolis Metropolitan Police Department (IMPD)
6. **Resolution 24-64: CDW-Government –** Candace Harris, Chief Financial Officer, Metropolitan Emergency Services Agency (MESA)
7. **Resolution 24-65: New Era Technology –** Kinley Weber, Director of Information Services, Marion County Sheriff's Office
8. **Resolution 24-66: BizStream, Inc –** Amitav Thamba, Chief Technology Officer, Marion Superior Court
9. **Resolution 24-67: MTS IntegraTRAK** – David Williams, Unified Communications Manager, ISA
10. **Resolution 24-68: ISA Access Control Policy** – Nicole Heatly-Holmes, Chief Information Security Officer, ISA
11. **Resolution 24-69: Judge Marc Rothenberg Recognition of Service –** Chairman Joseph O'Connor
12. **Resolution 24-70: Mr. Terry Morris Recognition of Service –** Chairman Joseph O'Connor

Discussion Items:

None

The next scheduled Information Technology Board meeting will be held January 28, 2025, at 9:30 a.m. in Room 260 of the City-County Building, 200 East Washington Street.

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Information Technology Board Meeting: Minutes

Roll Call:

IT Board Members Present

Mr. Joseph O'Connor	Marion County Assessor	Chairman
Secretary Barbara Lawrence	Marion County Treasurer	Secretary
Ms. Kate Sweeney Bell	Marion County Clerk	Voting Member
Chief Valerie Cunningham	Indianapolis Metropolitan Police Department	Voting Member
Col. James Martin	Marion County Sheriff's Office	Voting Member
Ms. Janae Rhoton	Deputy City Controller	Voting Member
Ms. Jane Richardson	Mayoral Appointee (Community)	Voting Member
Judge Marc Rothenberg	Marion Superior Court	Voting Member

Also Present

Mr. Collin Hill	Information Services Agency	Chief Information Officer
Mr. Ethan Hudson	Office of Corporation Counsel	Legal Counsel
Nicole Heatly-Holmes	Information Services Agency	Chief Information Security Officer
Jim Jarvis	Information Services Agency	Deputy Director, IT Strategy
Kevin Moore	Information Services Agency	Chief Operating Officer
Kate Kotan	Information Services Agency	Application Services Manager

IT Board Business:

Approval of the August 27, 2024, Meeting Minutes:

Ms. Barbara Lawrence made a motion to approve the August 27, 2024, IT Board minutes. The motion was seconded by Chief Valerie Cunningham and Colonel James Martin. A voice vote was called, and all consented with an aye vote. Having recorded the votes, the motion passed unanimously.

Status Updates:

Mr. Collin Hill, ISA CIO, presented the October 29, 2024, ISA Report.

Chief Financial Officer Kai Davis presented ISA's 3rd Quarter Financial Report and XBE data.

All reports and materials for this meeting are available for viewing in the October 29, 2024, Board Packet online at indy.gov/activity/information-technology-board.

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Information Technology Board Meeting: Minutes

Action Items:

Resolution 24-55: Vertosoft, LLC – Kate Kotan, Application Services Manager, ISA

The Information Services Agency ("ISA") sought approval from the IT Board to contract with Vertosoft, LLC ("Vertosoft") for OpenGov technology products, solutions and related services through the Omnia Partners agreement in an amount not to exceed Seven Hundred Thousand Dollars and Zero Cents ($750,000.00) for a three (3) year term.

Secretary Lawrence made a motion to approve Resolution 24-55. The motion was seconded by Chief Cunningham. The motion passed unanimously.

Resolution 24-56: Kofax Total Agility (EARC) – Kate Kotan, Application Services Manager, ISA

The Information Services Agency ("ISA") sought approval from the IT Board to approve an expenditure from the Enhanced Access Review Committee ("EARC") in an amount of One Hundred Fifty Thousand Dollars and Zero Cents ($150,000.00) for the purchase of Kofax TotalAgility licenses and related maintenance to provide more efficient data capture, automation and digital workflow management for various City-County agencies and departments.

Ms. Kate Sweeney Bell made a motion to approve Resolution 24-56, and the motion was seconded by Ms. Jane Richardson. The motion passed unanimously.

Resolution 24-57: Granicus, Inc. – Kevin Moore, Chief Operating Officer, ISA

The Information Services Agency "ISA") as the Television and Video Services Agency ("TVSA") sought approval from the IT Board to amend the current agreement with Granicus, Inc. ("Granicus") and raise the not to exceed amount by Three Hundred Seventeen Thousand, Five Hundred Eighty-Two Dollars and Ninety Cents ($317,582.90) for a revised not to exceed amount of Five Hundred Eighty-Seven Thousand, One Hundred Ninety-Seven Dollars and Fifteen Cents ($587,197.15) for four (4) years for managed services of hardware and software maintenance and support.

Secretary Lawrence made a motion to approve Resolution 24-57. It was seconded by Colonel James Martin and the motion passed unanimously.

Resolution 24-58: AT&T Mobility National Accounts, LLC – Kevin Moore, Chief Operating Officer, ISA

The Information Services Agency ("ISA") sought approval from the IT Board to enter into a new agreement with AT&T Mobility for Enterprise VPN and related services for a total amount not to exceed Four Hundred Eighty-Seven Thousand, One Hundred Thirteen Dollars and Zero Cents ($487,113.00) for three (3) years.

Ms. Kate Sweeney Bell made a motion to approve Resolution 24-58, and the motion was seconded by Secretary Lawrence. The motion passed unanimously.

Resolution 24-59: ISA Authorized Approver Policy – Nicole Heatly-Holmes, Chief Information Security Officer, ISA

The Information Services Agency ("ISA") sought approval from the IT Board for revisions to the current Authorized Approver Policy, which governs the selection of agency authorized approvers who have the ability to make decisions impacting their agency/department's finances or data security and have authorization to submit Security Requests.

Secretary Lawrence made a motion to approve Resolution 24-59, and the motion was seconded by Ms. Jane Richardson and Colonel James Martin. The motion passed unanimously.

Resolution 24-60: ISA Local Administrator Rights Policy - Nicole Heatly-Holmes, Chief Information Security Officer, ISA

The Information Services Agency ("ISA") sought approval from the IT Board for revisions to the current Local Administrator Rights Policy, which supports the goal of ensuring the highest level of stability and usability for end-user devices and servers to install applications or make changes to their devices. Local administrator rights are typically reserved for staff of the Information Services Agency ("ISA") but, in some cases, users who are not affiliated with ISA may be issued these rights.

Secretary Lawrence made a motion to approve Resolution 24-60. The motion was seconded by Colonel James Martin and the motion passed unanimously.

Resolution 24-61: ISA Enterprise Security Program Policy - Nicole Heatly-Holmes, Chief Information Security Officer, ISA

The Information Services Agency ("ISA") sought approval from the IT Board for revisions to the current Enterprise Security Program Policy, which governs the protection of the City-County's information, assets and operations from security threats and breaches, while ensuring confidentiality, integrity, and availability of data and systems. The policy provides a framework for establishing accountability and provides oversight to ensure organizational risks are adequately mitigated while also ensuring that controls are implemented to mitigate risks.

Secretary Lawrence made a motion to approve Resolution 24-61. The motion was seconded by Ms. Kate Sweeney Bell and the motion passed unanimously.

Resolution 24-62: Sarah Riordan Recognition of Service – Joseph O'Connor, IT Board Chair

Chairman O'Connor acknowledged the service of Ms. Sarah Riordan to the Information Technology Board ("IT Board") for the past one (1) year and five (5) months as a board member. Ms. Riordan was also recognized for her service to the City of Indianapolis and Marion County, where she served as Executive Director and General Counsel for the Indianapolis Local Public Improvement Bond Bank and, most recently, as City Controller.

Secretary Lawrence made a motion to approve Resolution 24-62. The motion was seconded by Ms. Janae Rhoton, and the motion passed unanimously.

Discussion Items:

Mr. Jim Jarvis offered a report on the Center for Digital Government Project Experience (GovX) Award for the Marion Superior Court Smart Courts Initiative that was presented to the Marion Superior Court and the Information Services Agency on September 19, 2024.

Meeting Adjournment

Secretary Lawrence entertained a motion to adjourn. The motion was seconded by Judge Marc Rothenberg and the meeting was adjourned.

The next scheduled Information Technology Board meeting is to be held on Tuesday, November 19, 2024, at 9:30 a.m. in City-County Building Room 260.

INFORMATION
SERVICES AGENCY
City of Indianapolis & Marion County

ISA IT Board Report

November 19, 2024

Enterprise Projects

Project	Phase	Target	Status
Unified Communications: Implementation – Phase III	Executing	12/31/2024	
CCB Restack Phase II	Executing	1/30/25	
Storage Modernization	Executing	3/31/25	
Property Tax Management RFP	Executing	TBD	
JMS Relaunch	Executing	7/25/25	
Enterprise GIS Upgrade	Executing	3/31/25	

Capital Projects

Project	Phase
Jail I	Completed
CJC: Youth Services Center	Executing
Solid Waste Garage	Planning
ACS Shelter	Planning
Grassy Creek Family Center	Implementation
IFD 32	Implementation
IFD 20	Design

Vendor Service Level Agreements

Service Level Agreements		August 2024	September 2024	October 2024
Bell Techlogix	**Number of SLAs**	**SLAs Achieved**	**SLAs Achieved**	**SLAs Achieved**
Service Desk / Cross Functional	35	35	35	35
Workplace	13	13	13	13
Data Center / Network	28	28	28	28
Daniels Associates, Inc. (DAI)	**Number of SLAs**	**SLAs Achieved**	**SLAs Achieved**	**SLAs Achieved**
Service	23	23	23	23
Personnel	3	3	3	3

Customer Satisfaction

INFORMATION
SERVICES AGENCY
City of Indianapolis & Marion County

2024 ISA Financial Report

Information Technology Board

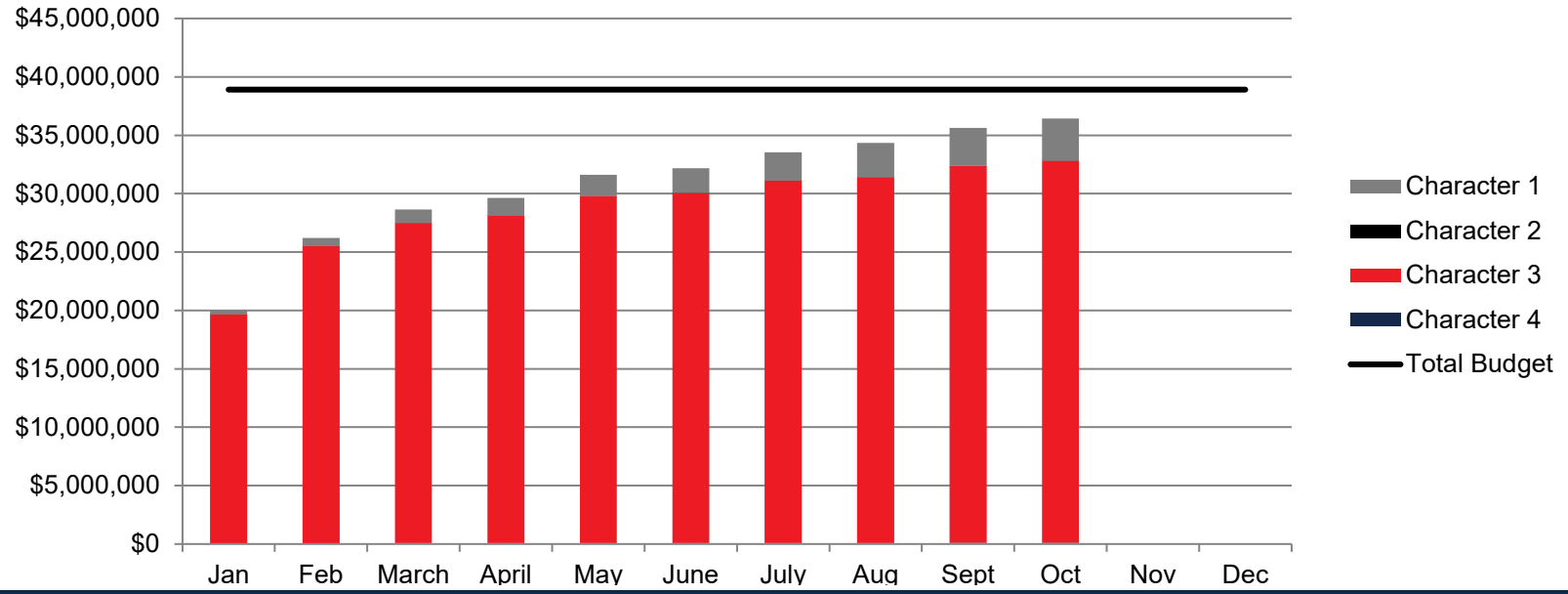
November 19, 2024

Kai Davis, Chief Financial Officer

Financial Management

2024 ISA YTD Expenses by Character

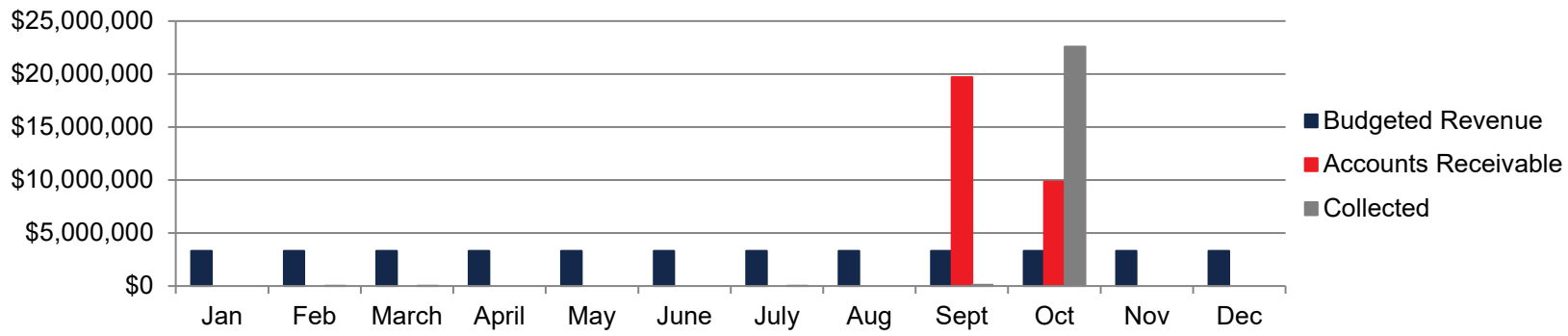
Character	2024 Budget	YTD Spend	Encumbered	Total $	Total %	Remaining Budget
Character 1: Personnel	$4,543,200	$3,576,023	$0	$3,576,023	78.71%	$967,177
Character 2: Supplies	$92,460	$18,616	$2,862	$21,478	23.23%	$70,982
Character 3: Services	$34,108,929	$25,645,277	$7,082,153	$32,727,430	95.95%	$1,381,499
Character 4: Capital	$170,000	$86,208	$11,336	$97,544	57.38%	$72,456
Total	**$38,914,589**	**$29,326,124**	**$7,096,351**	**$36,422,474**	**93.60%**	**$2,492,115**



Financial Management

2024 ISA YTD Revenue by Source

Revenue Source	Budget	Billed	% Billed	Collected	% Collected
Internal Chargeback	$39,457,392	$29,148,060	74%	$22,584,278	77%
External Chargeback	$293,620	$414,672	141%	$74,798	18%
Miscellaneous	$0	$0	N/A	$102,241	N/A
Total	**$39,751,012**	**$29,562,732**		**$22,761,317**	



INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Resolution 24-63

INFORMATION TECHNOLOGY BOARD

Resolution to Establish a Professional Services Agreement and Authorize Expenditure with Flock Group, Inc.

WHEREAS, Section 281-223 of the Revised Code of the Consolidated City of Indianapolis and Marion County empowers the Marion County Information Technology Board ("IT Board") to approve any information technology contracts funded by the City-County prior to contract execution; and

WHEREAS, the Indianapolis Metropolitan Police Department ("IMPD") seeks approval to contract with Flock Group, Inc., ("Flock Group") for the continued use of a situational awareness solution to create, view, search and archive footage on devices provided by IMPD, participating businesses and Flock Group; and

WHEREAS, the IMPD seeks approval from the IT Board to establish a Professional Services Agreement with Flock Group, Inc., for a total amount not to exceed Six Million Dollars and Zero Cents ($6,000,000.00); and

WHEREAS, the Information Services Agency ("ISA") recommends approval of the agreement with Flock Group, Inc; and

NOW THEREFORE BE IT RESOLVED, the IT Board authorizes the Indianapolis Metropolitan Police Department, subject to the ISA's Chief Information Officer approval, to enter into an agreement with Flock Group, Inc., in an amount not to exceed Six Million Dollars and Zero Cents ($6,000,000.00) for a four (4) year term.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Resolution 24-64

INFORMATION TECHNOLOGY BOARD

Resolution to Authorize Expenditure to CDW-Government, LLC

WHEREAS, Section 281-223 of the Revised Code of the Consolidated City of Indianapolis and Marion County empowers the Marion County Information Technology Board ("IT Board") to approve any information technology contracts funded by the City-County prior to contract execution; and

WHEREAS, the Metropolitan Emergency Services Agency ("MESA") seeks approval to contract with CDW-Government, LLC., ("CDW") for technology communication services, including the design, installation, maintenance support services and networking components to replace the video wallboard display at the Marion County Emergency Operations Center ("EOC"); and

WHEREAS, MESA seeks approval from the IT Board to enter into an agreement with CDW-Government, LLC., for a total amount not to exceed Nine Hundred Thousand Dollars and Zero Cents ($900,000.00); and

WHEREAS, the Information Services Agency ("ISA") recommends approval of the agreement with CDW-Government, LLC., for technology communications services;

NOW THEREFORE BE IT RESOLVED, the IT Board authorizes the Metropolitan Emergency Services Agency, subject to the ISA's Chief Information Officer approval, to enter into an agreement with CDW-Government, LLC., for technology communications services in an amount not to exceed Nine Hundred Thousand Dollars and Zero Cents ($900,000.00) for five (5) years.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Resolution 24-65

INFORMATION TECHNOLOGY BOARD

Resolution to Authorize Expenditure with New Era Technology for the Marion County Sheriff's Office

WHEREAS, Section 281-223 of the Revised Code of the Consolidated City of Indianapolis and Marion County empowers the Marion County Information Technology Board ("IT Board") to approve any information technology contracts funded by the City-County prior to contract execution; and

WHEREAS, the Marion County Sheriff's Office ("MCSO") seeks approval to contract with New Era Technology ("New Era") for technical support and on-site services for audiovisual systems and Vitec licensing support for the IP-TV system; and

WHEREAS, the MCSO seeks approval from the IT Board to enter into an agreement with New Era Technology for technical support and on-site services for audiovisual systems and Vitec licensing support for the IP-TV system for a total amount not to exceed Three Hundred Seventy-Six Thousand, One Hundred Ninety-Five Dollars and Zero Cents ($376,195.00); and

WHEREAS, the Information Services Agency ("ISA") recommends approval of the agreement with New Era Technology; and

NOW THEREFORE BE IT RESOLVED, the IT Board authorizes the Marion County Sheriff's Office, subject to the ISA's Chief Information Officer approval, to enter into an agreement with New Era Technology for technical support and on-site services for audiovisual systems and Vitec licensing support for the IP-TV system for a total amount not to exceed Three Hundred Seventy-Six Thousand, One Hundred Ninety-Five Dollars and Zero Cents ($376,195.00) for five (5) years.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Resolution 24-66

INFORMATION TECHNOLOGY BOARD

Resolution to Amend Agreement with BizStream, Inc., for the Marion Superior Courts Youth Services Center

WHEREAS, Section 281-223 of the Revised Code of the Consolidated City of Indianapolis and Marion County empowers the Marion County Information Technology Board ("IT Board") to approve any information technology contracts funded by the City-County prior to contract execution; and

WHEREAS, the Marion Superior Court ("MSC") currently contracts with BizStream, Inc., ("BizStream) for software and services for the Marion Superior Courts Youth Services Center case management system; and

WHEREAS, the MSC seeks approval from the IT Board to amend its agreement with BizStream and raise the not to exceed amount by Five Hundred Sixty-Five Thousand Dollars and Zero Cents ($565,000.00) for a revised total amount not to exceed One Million, Four Hundred Eighty-One Thousand, Seven Hundred Sixty-Three Dollars and Zero Cents ($1,481,763.00) for software and services, additional scope items and future enhancements; and

WHEREAS, the Information Services Agency ("ISA") recommends approval of the agreement with BizStream; and

NOW THEREFORE BE IT RESOLVED, the IT Board authorizes the Marion Superior Court, subject to the ISA's Chief Information Officer approval, to amend its agreement with BizStream in an amount not to exceed Five Hundred Sixty-Five Thousand Dollars and Zero Cents ($565,000.00) for a revised total amount not to exceed One Million, Four Hundred Eighty-One Thousand, Seven Hundred Sixty-Three Dollars and Zero Cents ($1,481,763.00) for software and services, additional scope items and future enhancements through December 31, 2028.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Resolution 24-67

INFORMATION TECHNOLOGY BOARD

Resolution to Amend Agreement with MTS IntegraTRAK, Inc., for Telecommunications Licenses, Services and Support

WHEREAS, Section 281-223 of the Revised Code of the Consolidated City of Indianapolis and Marion County empowers the Marion County Information Technology Board ("IT Board") to approve any information technology contracts funded by the City-County prior to contract execution; and

WHEREAS, the Information Services Agency ("ISA") currently contracts with MTS IntegraTRAK, Inc., ("MTS") for telecommunications licenses, services and support; and

WHEREAS, ISA seeks approval from the IT Board to amend its agreement with MTS and raise the not to exceed amount by Fifty Thousand Dollars and Zero Cents ($50,000.00) for a revised total amount not to exceed Two Hundred Sixty-Nine Thousand, Twelve Dollars and Forty Cents ($269,012.40); and

WHEREAS, the Information Services Agency ("ISA") recommends approval of the agreement with MTS IntegraTRAK for telecommunications licenses, services and support; and

NOW THEREFORE BE IT RESOLVED the IT Board authorizes the Information Services Agency, subject to the Chief Information Officer approval, to enter into an agreement with MTS IntegraTRAK, Inc., for telecommunications licenses, services and support in an amount not to exceed Fifty Thousand Dollars and Zero Cents ($50,000.00) for a revised total amount not to exceed Two Hundred Sixty-Nine Thousand, Twelve Dollars and Forty Cents ($269,012.40) for a one (1) year term.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

RESOLUTION 24-68

INFORMATION TECHNOLOGY BOARD

Resolution to Approve the Information Services Agency Access Control Policy with Remote Access

WHEREAS, the Information Technology Board ("IT Board") has the following powers and duties pursuant to Section 281-212 of the Revised Code of Indianapolis and Marion County:

- To establish and revise information technology guidelines, standards and benchmark processes for subject agencies and other users;

- To develop, maintain and communicate IT services policy and administrative procedures for users; and

WHEREAS, the Information Services Agency ("ISA") has drafted an Access Control Policy with Remote Access (attached) in order to ensure that access controls are implemented and in compliance with IT security policies, standards and procedures within the City of Indianapolis-Marion County information technology environment. The policy also establishes authorized and secure methods for remote access (portals, direct application access, remote system control, tunnelling) to City-County resources and services and ensure the confidentiality, integrity, and availability of data and systems while mitigating the risks associated with remote access.

WHEREAS, this policy applies to all City-County employees, contractors, vendors, consultants, temporary and other workers, including all persons affiliated with third parties that may have access to City-County network computer resources and any individual accessing the information and systems.

NOW THEREFORE BE IT RESOLVED that the IT Board approves the Access Control Policy set forth by ISA to be effective November 19, 2024.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

Information Services Agency (ISA) IT Policy: Access Control Policy with Remote Access

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

Table of Contents

Access Control Policy

Authority

The Information Technology Board (IT Board) has the following powers and duties pursuant to Section 281-212 of the Revised Code of Indianapolis and Marion County:

- To establish and revise information technology guidelines, standards and benchmark processes for subject agencies and other users; and
- To develop and oversee adherence to standards for security and confidentiality of all data, information, and telecommunication systems.

The City of Indianapolis-Marion County (City-County) depends on the integrity and availability of information systems and is committed to protecting such. Resolution 18-7 was approved by the IT Board on March 27, 2018. The resolution sets forth an executive mandate to formalize the Enterprise Security Program (ESP). This document supports the ESP.

Purpose

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

Reference

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 and NIST SP 800-63.

Scope

The policy is applicable to all City-County employees, contractors, vendors, consultants, temporary, and other workers at ISA, including all personnel affiliated with third parties that may have access to City-County network computer resources and any individual accessing the information and systems.

Policy

This policy is applicable to all departments and users of City-County resources and assets.

Account Management

Information Services Agency (ISA) will:

a. Identify and select the following types of information system accounts to support organizational missions and business functions such as individual, resource, business-to-business, authorization, and service.

b. Assign account managers for information system accounts.

c. Establish conditions for group and role membership.

d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

e. Require approvals by system owners (agency approvers) for requests to create information system accounts.

f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

g. Monitor the use of information system accounts.

h. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

i. Authorize access to the information system based on a valid access authorization or intended system usage.

j. Review accounts for compliance with account management requirements every 2 years.

k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

l. Employ automated mechanisms to support the management of information system accounts.

m. Ensure that the information system automatically disables temporary and emergency accounts after usage.

n. Ensure inactive accounts are disabled after 90 days.

o. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

Access Enforcement

ISA will:

a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

b. Ensure that all users utilize Multi-Factor Authentication (MFA) when accessing any City-County network services, systems, or devices.

Information Flow Enforcement

ISA will:

a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

Least Privilege

ISA will:

a. Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

b. Authorize explicit access to hardware and software, control access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

c. Require that users of information system accounts or roles with access to Security alerting software, Account management, Security-based policies and processes will use non-privileged accounts or roles when accessing non-security functions.

d. Restrict privileged accounts on the information systems to the CISO, Security Architect, Security Manager, Security Engineers/Analysts, and Data Center & Messaging Architect/Engineers.

e. Ensure that the information system audits the execution of privileged functions.

f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Unsuccessful Logon Attempts

ISA will ensure that the information system:

a. Enforces a limit of five (5) attempted consecutive invalid logon attempts by a user within a 15-minute window.

b. Locks the account/node automatically until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

System Use Notification

ISA will ensure that the information system:

a. Displays to users an approved System Use Notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

   i. Users are accessing a Security Information System.

ii. Information system usage may be monitored, recorded, and subject to audit.

iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

iv. Use of the information system indicates consent to monitoring and recording.

v. There are no rights to privacy.

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

c. For publicly accessible systems, the ISA will ensure that the information system:

i. Displays system use information on login, before granting further access.

ii. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

iii. Includes a description of the authorized uses of the system.

Session Lock

ISA will ensure that the information system:

a. Prevents further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.

b. Retain the session lock until the user re-establishes access using recognized identification and authentication procedures.

c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

Session Termination

ISA will:

a. Ensure that the information system automatically terminates a user session after logout.

Permitted Actions Without Identification or Authentication

ISA will:

a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

b. Document and provide supporting rationale in the security plan for user actions not requiring identification or authentication within an information system.

Remote Access

ISA will:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

b. Authorize remote access to the information system prior to allowing such connections.

c. Ensure that the information system monitors and controls remote access methods.

d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

e. Ensure that the information system routes all remote accesses through access control points to reduce the risk for external attacks.

f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for Administrators and those required for role.

g. Document the rationale for such access in the security plan for the information system.

h. Use a centrally managed authentication system for administration and user access.

i. Will review all devices and software used for remote access and must be approved by the Information Security Officer/designated security representative.

j. Ensure that remote access sessions must require re-authentication after 30 minutes of inactivity.

k. Ensure that remote access sessions must not last any longer than 24 hours.

l. Monitor (defined as keeping system-generated digital activity logs) for unauthorized remote connections, privileged account access, and other anomalous activity. If necessary, appropriate incident response actions should be taken as per the City-County Incident Response Policy.

m. Tunneling specific controls:

    a) Network controls regulating access to the remote access endpoint and between remote devices and networks are required.

    b) When a remote access device will have access to other networked devices on the internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

Approved Methods of Remote Access

Approved methods of remote access to systems are listed in order of preference.

a. **Portals** - A server that offers access to one or more applications through a single centralized interface that provides authentication (e.g., web-based portal, virtual desktop interface (VDI).

b. **Direct Application Access** - Accessing an application directly with the application providing its own security (e.g., webmail, https).

c. **Remote System Control** - Controlling a system remotely from a location other than the entity's internal network.

d. **Tunneling** - A secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN).

Required Controls for Remote Access

a. Any method of remote access must use a centrally managed authentication system for administration and user access.

b. Devices and software used for remote access must be approved after review by the Information Security Officer/designated security representative. Blanket approvals may be provided based on this review.

c. The authentication token used for remote access must conform to the requirements of the appropriate assurance level.

d. Remote access sessions must require re-authentication after 30 minutes of inactivity.

e. Remote access sessions must not last any longer than 24 hours.

f. The ISA (networking/security) must monitor (defined as keeping system-generated digital activity logs) for unauthorized remote connections, privileged account access, and other anomalous activity. If necessary, appropriate incident response actions should be taken as per the City-County Incident Response Policy.

g. Tunneling specific controls:

    c) Network controls regulating access to the remote access endpoint and between remote devices and networks are required.

    d) When a remote access device will have access to other networked devices on the internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

Wireless Access

ISA will:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

b. Authorize wireless access to the information system prior to allowing such connections.

c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

d. Maintain the captive portal to redirect users before gaining access to public Wi-Fi.

Access Control for Mobile Devices

ISA will:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

b. Authorize the connection of mobile devices to organizational information systems.

c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

Use of External Information Systems

ISA will:

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

    i. Access the information system from external information systems.

    ii. Process, store, or transmit organization-controlled information using external information systems.

b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

    i. Verifies the implementation of required security controls on the external system as specified in the City-County Information Security Policy and Security Plan.

ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Information Sharing

ISA will:

a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information based on the City-County Data Classification Policy.

b. Employ role-based access controls, or manual processes, as defined in established contracts and agreements with the requesting party to assist users in making information sharing and collaboration decisions.

Publicly Accessible Content

ISA will:

a. Designate individuals authorized to post information onto a publicly accessible information system.

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information, such as sensitive information, personally identifiable information, and criminal justice information.

c. Review the non-Criminal Justice Information Systems (CJIS) content on the publicly accessible information system for nonpublic information annually and remove such information, if discovered.

d. Review the CJIS content on the publicly accessible information system for nonpublic information quarterly and remove such information, if discovered.

Policy Compliance

ISA will verify compliance with this policy through various methods, including but not limited to network monitoring, business tool reports, internal and external audits, and feedback to ISA. If a user account or device is determined to be non-compliant with this policy in a way that poses a security risk, ISA may take actions to address the threat. Such actions include, but are not limited to, disabling user accounts, blocking IP addresses, and removing accounts and City-County data from devices. Any data that is confidential and found in an audit conducted by ISA will remain confidential and only be shared with that specific agency or department. Agencies and departments will not waive confidentiality rules by allowing ISA to perform audits.

As defined in the City-County Data Ownership Policy, under no circumstance is ISA considered the owner of any data originating in a different agency or department. ISA understands its role as custodian of data. Access, use, or release of agency or department data, by ISA, will only occur with the relevant agency or department's approval, or as required by law.

Exceptions

Requests for exceptions to this policy will be reviewed by the Chief Information Security Officer (CISO). Departments requesting exceptions will provide such requests to the CISO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the ISA, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CISO will review such requests and confer with the requesting department.

Non-Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge and civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Related Policies and Standards

Acceptable Use Policy
Data Ownership Policy
Data Classification Standard
Enterprise Security Program Policy

Policy Approval

Per Indianapolis Marion County Municipal Code Sec. 281-212.13, *the City of Indianapolis/Marion County IT Board has the power and authority to promulgate rules and regulations for the efficient administration of its policies and procedures for users.*

This policy has been reviewed and approved by the IT Board and will be enforced as of the effective date by the Chief Information Officer. It is the responsibility of all City-County IT users to always comply with this policy.

Policy Signatures:	
Joseph O'Connor, IT Board Chair	Collin Hill, Chief Information Officer
Date	Date

Disclaimer

This policy is subject to change without notice. ISA will make every effort to communicate any changes to the Enterprise via email notification. A current and complete list of ISA policies are maintained on the ISA Intranet site at http://gateway.indy.gov/sites/ISA/AboutISA/policies_procedures/Pages/default.aspx

Employee Acknowledgement of Access Control Policy

I acknowledge that I have read ISA's Access Control Policy in full and understand the terms of the policy and my responsibilities as a user and data owner, if applicable.

Participant Name (printed): _____

Participant Signature: _____

Date: _____

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

RESOLUTION 24-69

INFORMATION TECHNOLOGY BOARD

Resolution to Recognize Judge Marc Rothenberg for his service to the Information Technology Board

WHEREAS, Judge Rothenberg has served on the Information Technology Board from January 1, 2021, through December 31, 2024; and

WHEREAS, Judge Rothenberg has served as a board member on the Information Technology Board commendably and with excellent stewardship; and

WHEREAS, Judge Rothenberg has brought leadership, guidance and a strong sense of commitment to ensure the success of the Information Services Agency; and

WHEREAS, Judge Rothenberg also serves the City of Indianapolis-Marion County, most recently as Marion Superior Court Judge, Civil Division, and has held various judicial leadership roles within the Marion Superior Court since 2003; and

WHEREAS, the Information Technology Board would like to offer its sincere appreciation and thanks for his contributions and guidance during his tenure; and

NOW, THEREFORE, BE IT RESOLVED THAT the Information Technology Board extends recognition and appreciation to Judge Marc Rothenberg for his outstanding service to the City of Indianapolis and Marion County as a valued member of the Information Technology Board.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

INFORMATION SERVICES AGENCY
City of Indianapolis & Marion County

RESOLUTION 24-70

INFORMATION TECHNOLOGY BOARD

Resolution to Recognize Mr. Terry Morris for his service to the Information Technology Board

WHEREAS, Mr. Morris has served on the Information Technology Board from May 12, 2022, through December 31, 2024; and

WHEREAS, Mr. Morris has brought leadership, guidance and a strong sense of commitment to ensure the success of the Information Services Agency; and

WHEREAS, Mr. Morris has served as a board member on the Information Technology Board commendably and with excellent stewardship; and

WHEREAS, the Information Technology Board would like to offer its sincere appreciation for his contribution and guidance over the past two and a half (2.5) years; and

NOW, THEREFORE BE IT RESOLVED THAT the Information Technology Board extends recognition and appreciation to Mr. Terry Morris for his outstanding service to the City of Indianapolis and Marion County as a valued member of the Information Technology Board.

_____
Joseph O'Connor, Chairman
Information Technology Board

_____
Proxy for Barbara Lawrence, Secretary
Information Technology Board

November 19, 2024

ISA CONTRACT REPORT <$250,000
2024

Date Approved	Dept.	Description	Vendor	Annual $ Amount	Total $ Amount	MBE/WBE/VBE /DOBE	Notes
1/29/2024	ISA	Exsight Call Accounting	MTS Integra Trak Inc.		$219,012.00	No	Software/Maintenance
1/17/2024	ISA	Staffing augmentation	Technical Youth LLC		$125,000.00	No	IT Consulting
2/13/2024	DPW	Support and Maintenance of Fleet Services Database	Perpetual Technologies Inc		$133,920.00	Yes - VBE	Maintenance and Support
2/14/2024	ISA	Biometric and identity management for to Law Enforcement Operations	Tech5 USA Inc.		$64,075.00	No	Maintenance and Support
2/23/2024	ISA	Cloud Services for Website Calendar System	Brightly Software Inc.		$167,755.00	No	Software/Maintenance
2/26/2024	ISA	Cloud Services	Oracle America Inc.		$0.00	No	Master Agreement
3/7/2024	Forensic Services	STRmix Annual Upgrade	NicheVision Forensics LLC		$78,747.00	No	Software/Maintenance
3/7/2024	IFD	Application management	Inqremental LLC	$79,999.00	$94,998.00	No	Software/Maintenance
3/8/2024	MCSO	Credit Investigation and Reporting	Talx Corporation		$165,022.00	No	Universal Membership Agreement
4/8/2024	OFM	Oracle Enterprise Performance Management Cloud Remote Support	Innofin Solutions LLC		$60,000.00	No	Maintenance and Support
4/16/2024	MCSO	X-ray machine Maintenance services	Leidos Security Detection and Automation Inc.		$51,600.00	No	Maintenance and Support
4/15/2024	ISA	Tax Sale Platform	Govease Auction LLC		$215,000.00	No	Software/Maintenance
5/17/2024	MCSO	Inmate Telephone Services	Global Tel Link Corporation		$0.00	No	Outside Telephone Services
5/21/2024	OPHS	Datatelligent Data Analytics Subscription	Datatelligent LLC		$88,000.00	No	Subscription Services (SaaS)
5/28/2024	MCSO	software application hosting services and support	Hoover Blanket Inc. DBA Main Street Computing		$210,000.00	No	Software/Maintenance
5/29/2024	ISA	Mobility Premium Software Maintenance and Technical Support	AT&T Mobility		$236,254.00	No	Software/Maintenance
6/6/2024	ISA	On call services	Accela, Inc.		$200,000.00	No	Software Updating Services
6/10/2024	ISA	IDS Performane Coaching Executive Enrichment Program	Performance 3 LLC		$9,000.00	No	Software/Maintenance
6/14/2024	DBNS	Time and Materials	Accela, Inc.		$140,000.00	No	Support Services
7/2/2024	Marion Superior Courts	JURY+ Training System	Jury System Incorporated		$65,927.00	No	Software/Maintenance
7/2/2024	OFM	Online Plan Room and Plan Supply Services	Repro Graphix Inc		$0.00	Yes - WBE	Electronic Information and Mailing Services
7/15/2024	OEI	Salesforce Support Services	Crowe LLP		$10,000.00	No	Support Services
7/18/2024	OEI	Host and Administer the Enroll Indy School Finder and Onematch Application	Enroll Indy Inc		$150,000.00	No	Software, Maintenance, and Support
7/19/2024	MCSO	On-Call Services for Repairs and Parts	Astrophysics Inc		$107,127.00	No	X-Ray Equipment Maintenance and Repair
7/22/2024	Clerk's Office	FileNet P8 System	Berkone Inc		$137,484.00	No	Software/Maintenance
7/26/2024	ISA	Staffing augmentation	Technical Youth LLC		$188,440.00	No	IT Consulting
7/29/2024	Forensic Services	Maintenance and support of equipment	Qiagen Inc	$42,512.00	$163,582.00	No	Maintenance and Support
7/29/2024	IFD	Fire Simulation Training Software	Equipment Simulations LLC		$11,595.00	No	Software/Maintenance
7/29/2024	IMPD	Recruitment Website and Dashboard Development	Interview Now Inc		$27,500.00	No	Subscription Services (SaaS)
7/30/2024	ISA	Warranty for NVERZION System	Computer Engineering Inc		$13,194.00	No	Software/Maintenance
8/5/2024	OPHS	Door Access Control and Security Camera System Software	Tech Electronics of Indiana LLC		$40,000.00	No	Software, Maintenance, and Support
8/8/2024	OFM	Rev Q software	Columbia Ultimate Business Systems LLC		$29,000.00	No	Software/Maintenance
8/21/2024	DPR	Commission for Accreditation of Parks and Recreation Agencies (CAPRA)	PowerDMS Inc.		$40,000.00	No	Software/Maintenance
8/21/2024	Assessors Office	CoStar Software Platform	Costar Realty Information Inc		$119,593.04	No	Software/Maintenance
9/5/2024	MCSO	Various Software Licenses and Maintenance	Leads Online LLC		$35,178.00	No	Software/Maintenance
9/6/2024	IFD	Fire Engineering Training Premium Platform and Maintenance	Clarion Events Inc.		$113,125.00	No	Software/Maintenance
9/13/2024	ISA	E-learning and Interactive Online Training	Stormwind LLC		$52,000.00	No	Computer Based Training
9/17/2024	ISA	Agenda Meetings Management Essential Premium	CivicPlus LLC		$169,000.00	No	Software/Maintenance
10/18/2024	Human Resources	Software Services for Workplace Harrassment Reporting	HR Acuity LLC		$151,874.00	No	Software/Maintenance