AGENDA

LOS ANGELES REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEM AUTHORITY

JOINT OPERATIONS & TECHNICAL COMMITTEE MEETING

Tuesday, July 24, 2018 • 1:30 p.m.
LA-RICS Headquarters – Large Conference Room
2525 Corporate Place, Suite 200, Monterey Park, CA 91754

Los Angeles Regional Interoperable Communications System Authority (the "Authority")

AGENDA POSTED: July 20, 2018

Complete agendas are made available for review at the designated meeting location. Supporting documentation is available at the LA-RICS Office located at 2525 Corporate Place, Suite 200, Monterey Park, CA 91754 during normal business hours and may also be accessible on the Authority's website at http://www.la-rics.org.

OPERATIONS COMMITTEE

Members:

1. **John Geiger**, Los Angeles County, CEO
2. **Kyle Zuniga**, **Chair**, County of Los Angeles Fire Dept.
3. **Cathy Chidester**, Los Angeles County DHS
4. **Chris Donovan**, Los Angeles Area Fire Chiefs Association
5. **Anthony Vairo**, L.A. County Police Chiefs Association
6. **Tab Rhodes, Vice-Chair**, L.A. County Sheriff's Dept.
7. **John Curley**, Covina Police Dept.
8. **Jeff Steinhoff**, Inglewood Police Dept.
9. **Ron Sagmit**, Signal Hill Police Dept.
10. **Elliot Kase**, Alhambra Police Dept.

Alternates:

Mike Iwanaga, Los Angeles County, CEO
Chris Bundesen, County of Los Angeles Fire Dept**.**
Karolyn Fruhwirth, Los Angeles County DHS
Eric Zanteson, Los Angeles Area Fire Chiefs Association
Shelly Vander Veen, L.A. County Police Chiefs Association
Sven Crongeyer, L.A. County Sheriff's Department
Ric Walczak, Covina Police Dept.
Cardell Hurt, Inglewood Police Dept.
Brian Leyn, Signal Hill Police Dept.
Vacant, pending

TECHNICAL COMMITTEE

Members:

1. **John Geiger**, Los Angeles County, CEO
2. **Ted Pao**, **Chair**, Los Angeles County Internal Services Dept.
3. **Tab Rhodes**, Los Angeles County Sheriff's Dept.
4. **Jeffrey Morgan**, Los Angeles County DHS
5. **James Craig**, Manhattan Beach Fire Dept.
6. **Scott England**, **Vice-Chair**, County of Los Angeles Fire Dept.
7. **John Curley**, Covina Police Dept.
8. **Jeff Steinhoff**, Inglewood Police Dept.
9. **Ron Sagmit**, Signal Hill Police Dept.
10. **Elliot Kase,** Alhambra Police Dept.

Alternates:

Mike Iwanaga, Los Angeles County, CEO
Mike Dunning, Los Angeles County Internal Services Dept.
Sven Crongeyer, Los Angeles County Sheriff's Dept.
Kim Buard, Los Angeles County DHS
Eric Zanteson, Los Angeles Area Fire Chiefs Association
Rufino Fernandez, County of Los Angeles Fire Dept.
Ric Walczak, Covina Police Dept.
Cardell Hurt, Inglewood Police Dept.
Brian Leyn, Signal Hill Police Dept.
Vacant, pending

Officers:
Scott D. Edson, Executive Director

LA-RICS

NOTE: ACTION MAY BE TAKEN ON ANY ITEM IDENTIFIED ON THE AGENDA

I. CALL TO ORDER

II. ANNOUNCE QUORUM – Roll Call

III. APPROVAL OF MINUTES

A. May 22, 2018 – Regular Meeting Minutes

IV. PUBLIC COMMENTS

V. CONSENT CALENDAR – (None)

VI. REPORTS (B-C)

B. Status Report Update for LTE

C. Status Report Update for LMR

VII. DISCUSSION ITEMS (D)

Traveling Meeting Mobile

Agenda Item D

VIII. ADMINISTRATIVE MATTER (E)

E. APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS SECURITY POLICIES (POLICY NO. 025-2018 AND 026-2018)

It is recommended the Joint Operations and Technical Committees:

Approve a recommendation to the Board to adopt the following LA-RICS security policies to enhance the Authority's Information Technology (IT) Security Program:

- Board Policy No. 025-2018 – Use of LA-RICS Information Technology Resources Policy (Enclosure 1)

LA-RICS

- Board Policy No. 026-2018 – LA-RICS Antivirus Security Policy (Enclosure 2)

Agenda Item E

IX. MISCELLANEOUS – NONE

X. ITEMS FOR FUTURE DISCUSSION AND/OR ACTION BY THE COMMITTEE

XI. CLOSED SESSION REPORT - NONE

XII. ADJOURNMENT AND NEXT MEETING:

Tuesday, September 25, 2018, at 1:30 p.m., location forthcoming.

LA-RICS

COMMITTEE MEETING INFORMATION

Members of the public are invited to address the LA-RICS Committee on any item on the agenda prior to action by the Committee on that specific item. Members of the public may also address the Committee on any matter within the subject matter jurisdiction of the Committee. The Committee will entertain such comments during the Public Comment period. Public Comment will be limited to three (3) minutes per individual for each item addressed, unless there are more than ten (10) comment cards for each item, in which case the Public Comment will be limited to one (1) minute per individual. The aforementioned limitation may be waived by the Committee's Chair.

(NOTE: Pursuant to Government Code Section 54954.3(b) the legislative body of a local agency may adopt reasonable regulations, including, but not limited to, regulations limiting the total amount of time allocated for public testimony on particular issues and for each individual speaker.)

Members of the public who wish to address the Committee are urged to complete a Speaker Card and submit it to the Committee Secretary prior to commencement of the public meeting. The cards are available in the meeting room. However, should a member of the public feel the need to address a matter while the meeting is in progress, a card may be submitted to the Committee Secretary prior to final consideration of the matter.

It is requested that individuals who require the services of a translator contact the Committee Secretary no later than the day preceding the meeting. Whenever possible, a translator will be provided. Sign language interpreters, assistive listening devices, or other auxiliary aids and/or services may be provided upon request. To ensure availability, you are advised to make your request at least 72 hours prior to the meeting you wish to attend. (323) 881-8291 or (323) 881-8295

SI REQUIERE SERVICIOS DE TRADUCCION, FAVOR DE NOTIFICAR LA OFICINA CON 72 HORAS POR ANTICIPADO.

The meeting is recorded, and the recording is kept for 30 days.

JOINT OPERATIONS AND TECHNICAL COMMITTEES MEETING MINUTES

LOS ANGELES REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEM AUTHORITY

Tuesday, May 22, 2018 • 1:30 p.m.
LA-RICS Headquarters – Large Conference Room
2525 Corporate Place, Suite 200, Monterey Park, CA 91754

Operations Committee Members Present:
John Geiger, Los Angeles County, CEO
Shelly Vander Veen, L.A. County Police Chiefs Association
Jeff Steinhoff, Sergeant, City of Inglewood Police Department
Ric Walczak, Lieutenant, Covina Police Department
Elliot Kase, Assistant Chief of Police, Alhambra Police Department
Sven Crongeyer, Los Angeles County Sheriff's Department

Technical Committee Members Present:
Ted Pao, Chair, Information Technology Specialist, Los Angeles County Internal Services Department
John Geiger, Los Angeles County, CEO
Ric Walczak, Lieutenant, Covina Police Department
Jeffrey Morgan, Los Angeles County, DHS
Scott England, Vice Chair, Telecommunications Engineer Command and Control, LACoFD
Information Officer, EMS Agency, County of LADHS
Jeff Steinhoff, Sergeant, City of Inglewood Police Department
Elliot Kase, Assistant Chief of Police, Alhambra Police Department
Sven Crongeyer, Los Angeles County Sheriff's Department

Absent:
Kyle Zuniga, Chair, County of Los Angeles Fire Department
Judy Anderson, Vice-Chair, Lieutenant, Los Angeles County Sheriff's Department
Cathy Chidester, Los Angeles County, DHS
Chris Donovan, Los Angeles Area Fire Chiefs Association
Ron Sagmit, Lieutenant, Signal Hill Police Department
Steven Page, Los Angeles Area Fire Chiefs Association

Officers Present:
Scott D. Edson, LA-RICS Executive Director

AGENDA ITEM A

NOTE: ACTION MAY BE TAKEN ON ANY ITEM IDENTIFIED ON THE AGENDA

I. CALL TO ORDER

Technical Committee Chair Ted Pao called the meeting to order at 1:37 p.m.

II. ANNOUNCE QUORUM – Roll Call

Committee secretary Priscilla Lara took roll call for each committee and both committees had quorum.

III. APPROVAL OF MINUTES (A)

A. January 23, 2018 – Regular Meeting Minutes

Technical Committee Chair Ted Pao asked for a motion to approve the minutes. Committee Member unidentified moved to approve first, seconded by Technical Committee Vice Chair Scott England.

Ayes 9: Pao, Geiger, Vander Veen, Steinhoff, Walczak, Kase, Crongeyer, Morgan and England

IV. PUBLIC COMMENTS – (NONE)

V. CONSENT CALENDAR – (NONE)

VI. REPORTS (B-C)

B. Status Report Update for LTE

Eileen Healy, a consultant with Televate provided an update on the LTE Public Safety Broadband Network (PSBN). LA-RICS has agreement with AT&T to take over the existing 71 PSBN sites. The deal is targeted to close on or about July 1, 2018, pending NTIA approval. She provided some detail around the operational and technical aspects for this important network transition including completing the new LA-RICS Network Operations Center (NOC), user performance monitoring capabilities and agency connections to FirstNet/AT&T. Her presentation was following by a lively Q&A session where Committee Members asked questions about the LTE network transition. Questions included:

Will agencies become a customer of AT&T like anyone else? Technical Chair Pao stated any adopters of the FirstNet solution would become a customer of FirstNet/AT&T.

To what extent would we have a say in the operation of the network? Technical Chair Pao indicated that we expect continued access to user data and there will be some additional local control capability, which still needs additional information and definition. Project Director Chris Odenthal stated that the questions exist on the AT&T side and identified more areas that remain to be explored and clarified once the network is transitioned. Ms. Healy shared the performance dashboard that LA-RICS has developed and explained that LASD and LACoFD have requested that LA-RICS makes the dashboard available after the transition to AT&T.

The discussion then changed to the available County contract vehicles to purchase FirstNet services. Technical Vice Chair England asked as we migrate to FirstNet is there a state contract for pricing? Ms. Healy stated the request has been made to AT&T that if the agencies are using LA-RICS SIM to connect to the FirstNet Network there will be no service charge. Work is underway with the County of Los Angeles / ISD on a proper contract vehicle. Project Director Odenthal provided additional clarification on the pricing / adoption discussion. Additional questions were asked:

Is ISD contemplating procurement on behalf of Fire, Sheriff, the County or LA-RICS? Committee Member Sergeant Crongeyer stated ISD is conducting a local procurement for the County as a whole, but the FirstNet services being procured are only for Public Safety. Technical Vice Chair England commented he is concerned the terms and conditions for a local procurement / pricing will take quite some time.

C. Status Report Update for LMR

Program Manager Justin Delfino presented a PowerPoint Presentation to the attendees that included the following:

Program Manager Delfino provided a map/visual to illustrate sites that are in construction and those completed and provided details supporting the construction-related activities occurring at these sites to date.

Technical Chair Pao asked for an approximate count of how many sites are currently under construction? Program Manager Delfino stated that there are a total of 19 sites constructed, 17 of which are considered complete.

Construction completed sites are listed below:

1. TPK
2. BMT
3. MLM

4. PLM
5. MMC
6. HPK
7. ONK
8. LDWP243
9. CCT
10. LASDTEM
11. APC
12. CCB
13. MVS
14. PHN
15. SDW
16. FCCF
17. CLM

Under construction sites are listed below:

1. VPK
2. LA-RICS HQ

Given the timeline presented, Technical Vice Chair England asked when will we be able to come up with first simulcast cell?

Program Manager Delfino stated what is to be turned on will be determined by the Authority and policy decisions to be made.

Project Director Odenthal stated the individual sites can function by themselves. Pending backhaul connectivity to one of the cores. Most of the basin will be done by the end of the year. There are three sites that are necessary for the basin sites to turn on:

1. Rolling Hills
2. Baldwin Hills
3. Rio Hondo

Each of the sites under construction is expected to be completed by the end of this year or early next year. However, if there is a particular site that is needed prior to System Acceptance, the LA-RICS Board will need to make a policy decision regarding payment for operations and maintenance of a partial in the interest of public safety.

Technical Vice Chair England stated we had that MOU conversation before as far as bringing users on the system. He also requested further information as to the timeline contemplated.

Project Director Odenthal stated those sites are done with the exception of RHT (Rolling Hill Transmit), Signal Hill, and UCLA and you got everything in the mountain side and then Catalina in the south. We are adding east San Gabriel Valley, Pomona courthouse, and Industry. Pomona will be done by the end of the year; the site is on Pomona courthouse. LA-RICS (LMR buildout) is our charter. As this organization does not want to incur additional cost at this time to do early onboarding of agencies. If there is a reason to do something different for officer safety, we will consider that if an agency brings that forward.

Technical Chair Pao stated that we have being doing a lot of construction and a lot remains to be done. It's a big system and will take time to complete it.

VII. DISCUSSION ITEMS – (D)

D. LA-RICS LMR Fleet Mapping Workgroup

Committee Member Sergeant Crongeyer stated with all the work being done with the LMR system, there is a need to gather all the member agencies and discuss some fleet mapping issues, in particular, a channel (talkgroup) naming convention. Do we want to have some interoperable channels so Fire Department can talk to Fire Department only? Same for Law Enforcement only? Do we want to have just one big talk group? These are the questions that need to be answered and we would like to form a working group to discuss these issues and come up with some options within LA-RICS. We want to put out an invitation to all Member Agencies to participate in a working group so we can discuss these issues. We will extend that invitation and start producing some ideas for the committees to consider.

Committee Member Geiger stated that would be a good next step. Open the room and start discussion.

Project Director Odenthal asked, "Could you describe the qualifications you are looking for the working group member makeup?".

Member Sergeant Crongeyer stated we are looking for representatives with a general understanding of radio systems and their operation and why there is a need for fleet mapping/naming. We are looking for representatives that understand how their current radio system works.

Technical Chair Pao stated perhaps we would have mutual aid with other (none member) agencies.

Project Director Odenthal indicated that there may be some Members that participate in different communication system. We reported on a meeting with ICI and Motorola on how we are going to implement the ISSI. We identified Mt. Lee (as the preferred connection point) and looking at the timeline we expect to have some resolution in the next 30 days. the city of Los Angeles because it's at Mt. Lee. Having ICI participate or know about what we are doing could be useful. They are going to have to have similar mapping of channels for (interoperable) communication as LA-RICS.

Technical Chair Pao asked to take a step back to explain what ISSI is and how it would work between two systems.

Project Director Odenthal stated the ISSI system connects the two (P25) systems. If you are an ICI member and come into LA-RICS coverage area where there is lack of ICI coverage, you can use LA-RICS coverage and talk back to your dispatch center. LA-RICS Members will be able to do the same thing. You have to have the two networks working together so the people have to work together. Right now, from an approval Authority stand point, there is a discussion that Long Beach will have one (ISSI), LAPD and ICI will have one with LA-RICS serving as the hub and everyone connected to it. ICI group has a system up and running on a P25 platform.

Technical Chair Pao stated we are going to meet with ICI and other system operators on ISSI connections. Member Sergeant Crongeyer stated that sounds like a separate working group to discuss the ISSI and we can do that. It's going to have to be done. Project Director Odenthal responded that "yes" we are testing ISSI system with ICI probably in September 2018. Member Sergeant Crongeyer stated that we will put out for two working groups.

VIII. ADMINISTRATIVE MATTERS – (E-G)

E. APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS LAND MOBILE RADIO SYSTEM EARLY ONBOARDING POLICY (POLICY NO. 023-2018)

Deputy Program Manager Tanya Roth presented Agenda Item E and recommended that the JPA Board:

1. Approve recommendation to the Board of Policy No. 023-2018, LA-RICS LMR System Early Onboarding Policy and the corresponding LA-RICS LMR System Early Onboarding MOU which would ensure the Authority has a policy in place for use of the LMR System for operational purposes prior to Final LMR System Acceptance.

2. Approve recommendation to the Board to delegate authority to the Executive Director to execute MOUs with agencies interested in using the LMR System prior to Final LMR System Acceptance for operation and mission critical purposes.

3. Approve recommendation to the Board to delegate authority to the Executive Director to approve and execute amendments to the LMR System Early Onboarding MOU substantially similar in form to the attached at Enclosure 1, provided that they are approved as to form by Counsel to the Authority.

Member Sergeant Crongeyer asked if Counsel had reviewed the MOU, Deputy Program Manager Roth confirmed that Counsel had reviewed.

Contract Manager Jeanette Arismendez stated that the recommendation is to make the recommendation to the Board to request such delegation.

Member Geiger motioned first, seconded by Technical Vice Chair England.

Ayes 9: Pao, Geiger, Vander Veen, Steinhoff, Walczak, Kase, Crongeyer, Morgan and England

MOTION APPROVED

F. APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS INFORMATION TECHNOLOGY AND SECURITY PROGRAMPOLICY (POLICY NO. 024-2018)

Ms. Healy presented Agenda Item F and recommended that the JPA Board:

1. Approve a recommendation to adopt Board Policy No. 024-2018, LA-RICS Information Technology and Security Program Policy (Enclosure 1), that establishes a security program that ensures Authority Information Technology (IT) resources are protected against all forms of unauthorized access, use, disclosure, or modification.

Member Sergeant Crongeyer asked if these were policies for users for the LA-RICS IT system, LA-RICS computer and the software and the LMR networks system? Ms. Healy clarified that this policy if primarily for the LA-RICS staff, but all Member are expected to have similar policies.

Member Vander Veen motioned first, seconded by Member Sergeant Crongeyer.

Ayes 9: Pao, Geiger, Vander Veen, Steinhoff, Walczak, Kase, Crongeyer, Morgan and England

MOTION APPROVED

G. OPERATIONS COMMITTEE VICE CHAIR - ELECTION

Technical Chair Pao asked for a motion to approve recommendation be made to the Joint Operations and Technical Committee Members as follows:

Elect Lieutenant Tab Rhodes as the new Operations Committee Vice Chair.

Technical Vice Chair England motioned first, seconded by Member Sergeant Crongeyer.

Ayes 9: Pao, Geiger, Vander Veen, Steinhoff, Walczak, Kase, Crongeyer, Morgan and England

MOTION APPROVED

IX. MISCELLANEOUS – (NONE)

X. ITEMS FOR FUTURE DISCUSSION AND/OR ACTION BY THE COMMITTEE

XI. CLOSED SESSION REPORT – (NONE)

XII. ADJOURNMENT AND NEXT MEETING:

Technical Committee Chair Pao announced adjournment of this meeting at 2:26 p.m., and the next Committee Meeting is on Tuesday, July 24, 2018, at 1:30 p.m., at the LA-RICS Headquarters, 2525 Corporate Place, Monterey Park 91754, Suite 200 the Large Conference Room.

LOS ANGELES REGIONAL INTEROPERABLE
COMMUNICATIONS SYSTEM AUTHORITY
2525 Corporate Place, Suite 100
Monterey Park, California 91754
Telephone: (323) 881-8291
http://www.la-rics.org

SCOTT EDSON
EXECUTIVE DIRECTOR

July 24, 2018

Joint Operations and Technical Committee Members
Los Angeles Regional Interoperable Communications System Authority (the "Authority")

Dear Committee Members:

APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS' SECURITY POLICIES (POLICY NOS. 025-2018 AND 026-2018)

SUBJECT

Request from the Joint Operations and Technical Committees to recommend certain LA-RICS security Policies, attached hereto, be presented to the Joint Powers Authority (JPA) Board of Directors (Board) with a recommendation to approve and adopt the policies.

RECOMMENDED ACTIONS

It is recommended the Joint Operations and Technical Committees:

Approve a recommendation to the Board to adopt the following LA-RICS security policies to enhance the Authority's Information Technology (IT) Security Program:

- Board Policy No. 025-2018 – Use of LA-RICS Information Technology Resources Policy (Enclosure 1)

- Board Policy No. 026-2018 – LA-RICS Antivirus Security Policy (Enclosure 2)

BACKGROUND

On May 22, 2018, your Committees approved a recommendation to adopt Policy No. 024-2018 (LA-RICS Information Technology and Security Program Policy) that

established a security program to ensure that the Authority's IT resources are protected against all forms of unauthorized access, use, disclosure, or modification. Policy No. 024-2018 was the first policy, in a series of policies, presented to your Committees as part of the Authority's IT Security Program. If the recommended action is approved, the policies will be presented to the Board for consideration and also make up part of the Authority's IT Security Program.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Approval of the recommended action will move the items to the Board for consideration and adoption for inclusion into the Authority's IT Security Program for the protection and use of Authority IT Resources.

It is necessary to implement Policy No. 025-2018 (Use of LA-RICS Information Technology Resources Policy) to ensure that the use of Authority's IT Resources do not allow any forms of unauthorized access, use, disclosure, or modification. As opposed to Board Policy No. 024-2018, previously approved by your Committees for Board consideration, which defines the overarching LA-RICS IT Security Program, this policy holds the User accountable when using the Authority's IT Resources and expects the User to utilize IT Resources in a responsible, professional, ethical, and lawful manner. In addition, this policy defines measures that the Authority would adhere to in order to protect its IT Resources, including but not limited to, establishing access control mechanisms and determining appropriate User authentication levels.

With respect to Policy No. 026-2018 (LA-RICS Antivirus Security Policy), this policy is necessary in order to allow for the Authority's Chief Information Security Officer (CISO) to provide LA-RICS-approved real-time virus protection for all LA-RICS hardware and software to minimize risk to the Authority's IT Resources. Further, this policy prohibits Users from introducing malicious devices onto any IT Resources as well as disabling, modifying, or deleting computer security software.

Authority staff is working to develop subsequent security policies that will become part of the Authority's IT Security Program to present to this Joint Operations and Technical Committees for consideration. The expectation is to secure Joint Operations and Technical Committees' approval for these policies as well as other security policies that may be interrelated and present cohesive policies packages to the Board for approval. As a result, in the coming meetings, your Committees may see more of these IT security policies presented for consideration.

FISCAL IMPACT/FINANCING

The activity contemplated in the recommended action has no fiscal impact at this time.

FACTS AND PROVISIONS/LEGAL REQUIREMENT

Counsel to the Authority has reviewed the recommended action.

CONCLUSION

Upon the Committees' approval of the recommended action, Authority staff will present the policies to the Board coupled with additional interrelated security policies previously approved by your Committees for Board adoption and implementation.

Respectfully submitted,

SCOTT EDSON
EXECUTIVE DIRECTOR

JA
M:\LA-RICS POLICIES\Policy No. 025-2018 (Use of LA-RICS Information Technology Resources Policy)\Joint Ops and Tech\1 Tech Ops Letter_LARICS Info Tech and Antivirus Policies.docx

Enclosures

c: Counsel to the Authority

LA-RICS POLICIES

POLICY TITLE		POLICY NO.
Use of LA-RICS Information Technology Resources Policy		025-2018
APPROVED BY	**EFFECTIVE DATE**	**DATE LAST REVISED**
LA-RICS JPA Board of Directors	---	---

1.0 PURPOSE

To establish a policy for use of Authority Information Technology Resources which will ensure that they are protected against all forms of unauthorized access, use, disclosure, or modification.

2.0 DEFINITION REFERENCE

As used in this Policy No. 025-2018, the following terms shall have the same meaning as set forth in Policy No. 024-2018 LA-RICS Information Technology and Security Program.

- Authority IT Resources, hereinafter referred to as “IT Resources”
- Authority IT Security, hereinafter referred to as “IT Security”
- Authority IT User, hereinafter referred to as “User”
- Chief Information Security Officer, hereinafter referred to as “CISO”
- Computing devices
- Confidential Information
- Personal Information
- Systems

3.0 POLICY

All Users shall adhere to this Policy 025-2018 and sign the Los Angeles Regional Interoperable Communications System (LA-RICS) Agreement for Acceptable Use and Confidentiality of LA-RICS Information Technology Resources (Enclosure) prior to being granted access to IT Resources.

Users cannot expect any right to privacy concerning their activities related to IT Resources, including, without limitation, in anything they create, store, send, or receive using IT Resources. Having no expectation to any right to privacy includes, for example, that Users' access and use of IT Resources may be monitored or investigated by authorized persons at any time, without notice or consent.

Activities of Users may be logged and stored, may become public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time.

IT Resources may not be used:

a. For any unlawful purpose;
b. For any purpose detrimental to LA-RICS or its interests;
c. For personal financial gain;
d. In any way that undermines or interferes with access to or use of IT Resources for official LA-RICS purposes;
e. In any way that hinders productivity, efficiency, customer service, or interferes with a User's performance of official job duties;
f. To express or imply sponsorship or endorsement by LA-RICS, except as approved in accordance with LA-RICS' policies, standards, and procedures; or
g. For personal purpose where activities are for private gain or advantage, or an outside endeavor not related to LA-RICS business purpose. Personal purpose does not include the incidental and minimal use of IT Resources, such as occasional use of the internet.

No User shall intentionally, nor through negligence or damage, interfere with the operation of, or prevent authorized access to IT Resources. It is every User's duty to access and use IT Resources responsibly, professionally, ethically, and lawfully. The CISO has the right to administer access and use of all IT Resources including, without limitation, the right to monitor Internet, electronic communications (e.g., email, text messages, etc.), and data access. Access to IT Resources is a privilege and may be modified or revoked at any time, without notice or consent.

Monitoring access and use of IT Resources by Users must be approved in accordance with applicable policies and laws on investigations. If any evidence of violation is identified, the CISO must be notified immediately.

3.1 Access Control

Access control mechanisms shall be in place to protect against unauthorized access, use, exposure, disclosure, modification, or destruction of IT Resources. Such mechanisms may include, without limitation, hardware, software, storage media, policy and procedures, and physical security.

3.2 Authentication

Access to all Systems shall have an appropriate User authentication mechanism based on the sensitivity and level of risk associated with the information. All Systems containing information that require restricted access shall require User authentication before access is granted.

Users shall be responsible for integrity of the authentication mechanism granted to them. For example, Users shall not share their computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards). Furthermore, representing oneself as someone else, real or fictional, or sending information anonymously is prohibited unless specifically authorized by the CISO.

Fixed passwords or single-factor authentication, which are used for most access authorization, shall be changed at a frequency determined by the CISO.

Two-factor authentication is required for remote access and system administrator access to critical servers where Personal Information, Confidential Information, or otherwise sensitive information exists unless otherwise approved by the Executive Director.

3.3 Information Integrity

Users are responsible for maintaining the integrity of information that is part of IT Resources. They shall not knowingly or through negligence cause such information to be modified or corrupted in any way that would compromise accuracy or prevent authorized access.

3.4 Accessing IT Resources Remotely

Remote access to IT Resources by Users shall require approval by the CISO. Each User shall comply with, and only use equipment that complies with all applicable IT Security policies.

Without limiting the foregoing, Users who are authorized to remotely access IT Resources using personally owned computing devices shall ensure that the following are up to date on their personal device:

a. Antivirus software
b. Operating system software
c. Application software (e.g., critical updates and service packs)
d. Firewall (e.g., software and hardware firewalls)

3.5 Privacy

Information that is accessed using IT Resources shall be used in accordance with LA-RICS policies, standards, and procedures. Such information shall not be exposed or disclosed to unauthorized individuals.

3.6 Confidentiality

Unless specifically authorized by the Executive Director, sending, disseminating, or otherwise exposing and/or disclosing Personal and/or Confidential Information is strictly prohibited. This includes, without limitation, information that is subject to HIPAA, the HITECH Act, or any other confidentiality or privacy legislation.

4.0 COMPLIANCE

Authority personnel who violate this Policy No. 025-2018 may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-Authority personnel who violate this Policy No. 025-2018 may be subject to termination of contractual agreements, denial of access to IT Resources, and other actions as appropriate (e.g., cure letter), as well as both civil and criminal penalties.

5.0 POLICY EXCEPTIONS

Requests for exceptions to this Policy No. 025-2018 shall be reviewed by the CISO and shall require approval by the Executive Director. Users requesting exceptions shall provide such requests to the CISO.

The request should specifically state the following:

a. Scope and justification for the exception
b. Potential impact or associated risk upon granting the exception
c. Risk mitigation measures to be undertaken by the Authority
d. Initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein

The CISO shall review such requests, confer with the requestor, and refer the matter to the Executive Director for action.

References:

- LA-RICS Policy No. 024-2018 (Information Technology and Security Program Policy)
- Comprehensive Computer Data Access and Fraud Act, California Penal Code Section 502
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- California Civil Code Section 1798.29

LOS ANGELES REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEM (LA-RICS) AGREEMENT FOR ACCEPTABLE USE AND CONFIDENTIALITY OF LA-RICS INFORMATION TECHNOLOGY RESOURCES

As a Los Angeles Interoperable Communications System (LA-RICS) staffer on loan from my member agency, contractor, subcontractor, volunteer, or other authorized user ("Authority IT User") of Authority Information Technology (IT) Resources as defined herein, I understand that I occupy a position of trust. Furthermore, I shall use Authority IT Resources in accordance with LA-RICS policies, standards, and procedures. I understand that Authority IT Resources shall not be used:

- For any unlawful purpose;
- For any purpose detrimental to the LA-RICS or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of Authority IT Resources for official LA-RICS purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a Authority IT User's performance of his/her official job duties.

I shall maintain the confidentiality of Authority IT Resources (e.g., business information, personal information, and confidential information).

This Agreement is required by LA-RICS Policy No. 025-2018 Use of LA-RICS Information Technology Resources, which may be consulted directly.

As used in this Agreement, the term "Authority IT Resources" includes, without limitation, computers, systems, networks, software, and data, documentation and other information, owned, leased, managed, operated, or maintained by, or in the custody of, the LA-RICS or non-LA-RICS entities for LA-RICS purposes. The definitions of the terms "Authority IT Resources", "Authority IT User", "Authority IT Security Incident", "computing devices", "Personal information" and "Confidential information" are fully set forth in LA-RICS No. 024-2018 Information Technology and Security Program Policy.

As an Authority IT User, I agree to the following:

1. Computer crimes: I am aware of California Penal Code Section 502(c) – Comprehensive Computer Data Access and Fraud Act (set forth, in part, below). I shall immediately report to my management any suspected misuse or crimes relating to Authority IT Resources or otherwise.

2. No Expectation of Privacy: I do not expect any right to privacy concerning my activities related to Authority IT Resources, including, without limitation, in anything I create, store, send, or receive using Authority IT Resources. I understand that having no expectation to any right to privacy includes, for example, that my access and use of Authority IT Resources may be monitored or investigated by authorized persons at any time, without notice or consent.

3. Activities related to Authority IT Resources: I understand that my activities related to Authority IT Resources (e.g., email, instant messaging, blogs, electronic files, Authority Internet services, and Authority systems) may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall not either intentionally, or through negligence, damage, interfere with the operation of Authority IT Resources. I shall neither, prevent authorized access, nor enable unauthorized access to Authority IT Resources responsibly, professionally, ethically, and lawfully.

4. Authority IT Security Incident reporting: I shall notify the Chief Information Security Officer (CISO) as soon as an Authority IT Security Incident is suspected. An "Authority IT Security Incident" is defined as, per Board Policy No. 024-2018, LA-RICS Information Technology and Security Program Policy, any actual or suspected adverse event (e.g., virus/worm attack, exposure, loss, or disclosure of personal information and/or confidential information, disruption of data or system integrity, and disruption or denial of availability) relating to any Authority IT Security.

5. Security access controls: I shall not subvert or bypass any security measure or system which has been implemented to control or restrict access to Authority IT Resources and any related restricted work areas and facilities. I shall not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards).

6. Passwords: I shall not keep or maintain any unsecured record of my password(s) to access Authority IT Resources, whether on paper, in an electronic file, or otherwise. I shall comply with all LA-RICS policies relating to passwords. I shall immediately report to my management any compromise or suspected compromise of my password(s) and have the password(s) changed immediately.

7. Business purposes: I shall use Authority IT Resources in accordance with LA-RICS policies, standards, and procedures.

8. Confidentiality: I shall not send, disseminate, or otherwise expose or disclose to any person or organization, any personal and/or confidential information, unless specifically authorized to do so by LA-RICS management. This includes, without limitation, information that is subject to Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act of 2009, or any other confidentiality or privacy legislation.

9. Computer virus and other malicious devices: I shall not intentionally introduce any malicious device (e.g., computer virus, spyware, worm, key logger, or malicious code), into any Authority IT Resources. I shall not use Authority IT Resources to intentionally introduce any malicious device into any Authority IT Resources or any non-Authority IT systems or networks. I shall not disable, modify, or delete computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) on Authority IT Resources. I shall notify the

CISO as soon as any item of Authority IT Resources is suspected of being compromised by a malicious device.

10. Offensive materials: I shall not access, create, or distribute (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on Authority IT Resources (e.g., over Authority-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I shall report to my management any offensive materials observed or received by me on Authority IT Resources.

11. Internet: I understand that the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use Authority Internet services in accordance with Authority policies and procedures. I understand that my use of Authority Internet services may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall comply with all Authority Internet use policies, standards, and procedures. I understand that Authority Internet services may be filtered, but in my use of them, I may be exposed to offensive materials. I agree to hold the Authority harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive materials.

12. Electronic Communications: I understand that Authority electronic communications (e.g., email, text messages, etc.) created, sent, and/or stored using Authority electronic communications systems/applications/services are the property of the Authority. All such electronic communications may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time, without notice or consent. I shall comply with all Authority electronic communications use policies and use proper business etiquette when communicating over Authority electronic communications systems/applications/services.

13. Public forums: I shall only use Authority IT Resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) in accordance with LA-RICS policies, standards, and procedures.

14. Internet storage sites: I shall not store Authority information (i.e., personal, confidential (e.g., social security number, medical record), or otherwise sensitive (e.g., legislative data)) on any Internet storage site in accordance with LA-RICS policies, standards, and procedures.

15. Copyrighted and other proprietary materials: I shall not copy or otherwise use any copyrighted or other proprietary Authority IT Resources (e.g., licensed software and documentation, and data), except as permitted by the applicable license agreement

and approved by the Authority's Executive Director. I shall not use Authority IT Resources to infringe on copyrighted material.

16. Compliance with LA-RICS ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable LA-RICS ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements relating to Authority IT resources. These include, without limitation, 024-2018 Technology and Security Program Policy, 025-2018 Use of LA-RICS Information Technology Resources.

17. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision of this Agreement may result in disciplinary action and other actions (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that LA-RICS may seek all possible legal redress.

CALIFORNIA PENAL CODE SECTION 502(c)
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code Section 502(c) is incorporated in its entirety into this Agreement by reference, and all provisions of Penal Code Section 502(c) shall apply. For a complete copy, consult the Penal Code directly at website www.leginfo.legislature.ca.gov/.

502(c) Any person who commits any of the following acts is guilty of a public offense:

1. Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

2. Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

3. Knowingly and without permission uses or causes to be used computer services.

4. Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

5. Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

6. Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

7. Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

8. Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

9. Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Authority IT User's Name	Authority IT User's Signature
Authority IT User's Employee/ID Number	Date
Supervisor's Name	Supervisor's Signature
Manager's Title	Date

LA-RICS POLICIES

POLICY TITLE		POLICY NO.
LA-RICS Antivirus Security Policy		026-2018
APPROVED BY	**EFFECTIVE DATE**	**DATE LAST REVISED**
LA-RICS JPA Board of Directors	---	---

1.0 PURPOSE

To establish an antivirus security policy for the protection of all Authority IT Resources.

2.0 DEFINITION REFERENCE

As used in this Policy No. 026-2018, the following terms shall have the same meaning as set forth in LA-RICS Policy No. 024-2018 Information Technology and Security Program.

- Authority IT Resources, hereinafter referred to as “IT Resources”
- Authority IT Security, hereinafter referred to as “IT Security”
- Authority IT Security Incident, hereinafter referred to as “IT Security Incident”
- Authority IT User, hereinafter referred to as “User”
- Chief Information Security Officer, hereinafter referred to as “CISO”
- Computing devices

3.0 POLICY

The CISO shall provide LA-RICS-approved real-time virus protection for all LA-RICS hardware and software environments to mitigate risk to IT Resources. Antivirus software shall be configured to actively scan all files received by computing devices. Changes to the antivirus software configurations shall only be made, as needed, by authorized personnel.

Further, the CISO shall establish procedures ensuring that:

a. Computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) is updated when a new detection definition file, detection engine, software update (e.g., service packs and upgrades), and/or software version release, as

applicable, is available, and only once hardware/software compatibility is confirmed

b. Users who maintain direct Internet access shall implement an antivirus system to scan Internet web pages, emails, and File Transfer Protocol (FTP) downloads

c. Notification of IT Security Incidents comply with requirements of the LA-RICS Cybersecurity Incident Response Plan

Users shall comply with, and only use equipment (e.g., LA-RICS-owned computing devices and personally owned computing devices) that complies with all applicable LA-RICS IT security policies.

Users are prohibited from intentionally introducing any malicious device (e.g., computer virus, spyware, worm, and malicious code) into any IT Resource. Further, Users are prohibited from using IT Resources to intentionally introduce any malicious device into any IT Resources or any non-LA-RICS IT systems or networks.

Users are prohibited from disabling, modifying, or deleting computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) IT Resources.

Each User is responsible for notifying the CISO as soon as any IT Resource is suspected of being compromised by a malicious device.

If there is a conflict between an LA-RICS security policy and an LA County policy, the County policy will supersede the LA-RICS policy.

4.0 COMPLIANCE

Authority personnel who violate this Policy No. 026-2018 may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-Authority personnel who violate this Policy No. 026-2018 may be subject to termination of contractual agreements, denial of access to IT Resources, and other actions as appropriate (ie: cure letter), as well as both civil and criminal penalties.

5.0 POLICY EXCEPTIONS

Requests for exceptions to this Policy No. 026-2018 shall be reviewed by the CISO and shall require approval by the Executive Director. Users requesting exceptions shall provide such requests to the CISO.

The request should specifically state the following:

a. Scope and justification for the exception
b. Potential impact or associated risk upon granting the exception
c. Risk mitigation measures to be undertaken by the Authority
d. Initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein

The CISO shall review such requests, confer with the requestor, and refer the matter to the Executive Director for action.

References:

- LA-RICS Policy No. 021-2017 (Cybersecurity Incident Response)
- LA-RICS Policy No. 024-2018 (Information Technology and Security Program)
- LA-RICS Policy No. 025-2018 (Use of Information Technology Resources, including the Acceptable Use Agreement)