Agenda Item

AGENDA STAFF REPORT

ASR Control 23-000504

MEETING DATE:	06/27/23
LEGAL ENTITY TAKING ACTION:	Board of Supervisors
BOARD OF SUPERVISORS DISTRICT(S):	5
SUBMITTING AGENCY/DEPARTMENT:	John Wayne Airport (Pending)
DEPARTMENT CONTACT PERSON(S):	Charlene V. Reynolds (949) 252-5183
	Kim Kitko (949) 252-5291

SUBJECT: Approve Amendment One for Wireless Public Internet Access Agreement

CEO CONCUR	COUNTY COUNSEL REVIEW	CLERK OF THE BOARD
Pending Review	Pending Review	Discussion 4/5 Vote

Budgeted: Yes **Current Year Cost:** N/A **Annual Cost:** N/A

Staffing Impact: No **# of Positions:** **Sole Source:** No

Current Fiscal Year Revenue: See Financial Impact Section

Funding Source: N/A **County Audit in last 3 years:** No

Levine Act Review Completed: Yes

Prior Board Action: 2/25/2014 #31

RECOMMENDED ACTION(S):

Approve and execute Amendment Number One to the Wireless Public Internet Access and Distributed Antenna System Agreement with Concourse Communications, LLC, to extend the term effective August 1, 2023, through July 31, 2033.

SUMMARY:

Approval of Amendment Number One to the Wireless Public Internet Access and Distributed Antenna System Agreement with Concourse Communications, LLC will provide continuity of service and elevate wireless performance with a system upgrade.

BACKGROUND INFORMATION:

Concourse Communications Group, LLC (a subsidiary of Boingo) is a privately-owned company with over 350 full-time staff members. Boingo is the largest independent provider of indoor Distributed Antenna System (DAS) in the United States, with more than 44,000 deployments in large-scale venues. Boingo has more than 21 years of experience and is the leader in the design, installation, operation, maintenance, and marketing of neutral host cellular DAS and public/private wireless fidelity (Wi-Fi)

networks in densely populated venues spanning airports, commercial real estate properties, stadiums, arenas, and military bases.

In 2014, John Wayne Airport (JWA) released a Request for Proposals (RFP) for Wireless Public Internet Access and DAS, and on February 25, 2014, the Board of Supervisors (Board) authorized to execute the Wireless Public Internet Access and DAS Operating Agreement (Agreement) with Concourse Communications Group, LLC (Boingo).

On June 2, 2021, pursuant to Section 2.02 of the Agreement, the County of Orange (County) exercised its option to extend the term one additional year, effective August 1, 2021, through July 31, 2022.

On May 25, 2022, pursuant to Section 2.02 of the Agreement, the County exercised its option to extend the term one additional year, effective August 1, 2022, through July 31, 2023.

In 2019, Boingo deployed a trial launch to test the next generation of Wi-Fi capabilities at JWA, the first Wi-Fi 6 deployment at a major airport. Wi-Fi 6 is a new industry standard developed to advance Wi-Fi capabilities to effectively handle growing traffic demands.

PROPOSED AMENDMENT:

Within the first year of the proposed Amendment, Boingo will ensure continuity of service and improve wireless performance at JWA by upgrading the Wi-Fi system to Wi-Fi 6 and committing a capital investment of $1.49 Million. The proposed Amendment also expands the existing coverage area to rideshare pick-up and drop-off areas located in Parking Structure A2, Parking Structure B2, Parking Structure C, the Customs and Border Protection area and Main Street Parking Lot as approved by the Airport Director. By year three of the extension, Boingo will complete a full upgrade of the neutral host DAS to 5G for all carriers. The proposed Amendment also requires Boingo to provide a minimum of $300,000 in additional network upgrades over the ten-year extension, as approved by the Airport Director, to address coverage gaps and to align with current technology and industry standards.

JWA reviewed Boingo's proposal and recommends extending the Agreement to ensure non-interruption of services and decrease infrastructure improvement impacts over the course of the next few years.

Compliance with CEQA:
The proposed project was previously determined to be Categorically Exempt from CEQA pursuant to Section 15301 (Class 1) of the CEQA Guidelines, on February 25, 2014, when it was originally approved because the Amendment consists of maintenance or minor alteration of existing public structures, mechanical equipment, involving negligible expansion of existing use. The proposed project is still consistent with this determination.

FINANCIAL IMPACT:

Revenues related to the concession lease are included in Fund 280, Airport Operating Fund, FY 2023-24 Budget, and will be included in the budgeting process for future years.

The revenue to JWA for Boingo's Lease Term of August 1, 2023, through July 31, 2033, will be $1,500,000.

STAFFING IMPACT:

N/A

ATTACHMENT(S):

Attachment A – Amendment Number One with Concourse Communications, LLC

AMENDMENT NUMBER ONE TO WIRELESS PUBLIC INTERNET ACCESS AND DISTRIBUTED ANTENNA SYSTEM AGREEMENT

THIS FIRST AMENDMENT TO WIRELESS PUBLIC INTERNET ACCESS AND DISTRIBUTED ANTENNA SYSTEM ("First Amendment") is made and entered into as of _____, 2023, by and between the COUNTY OF ORANGE, a political subdivision of the State of California ("County") and CONCOURSE COMMUNICATIONS GROUP, LLC ("Operator"). County and Operator may sometimes hereinafter individually be referred to as "Party" or jointly as "Parties."

RECITALS

WHEREAS, County and Operator entered into a Wireless Public Internet Access and Distributed Antenna System Agreement, dated February 25, 2014 ("Existing Agreement"); and

WHEREAS, County, through its Board of Supervisors, is the owner and proprietor of John Wayne Airport ("JWA" or "Airport"), located in the County of Orange, State of California, and operates and maintains the Airport as a governmental function for the primary purpose of providing air transportation to the public; and

WHEREAS, on June 2, 2021, pursuant to Section 2.02 of the Existing Agreement, County exercised its option to extend the term one additional year, effective August 1, 2021 through July 31, 2022; and

WHEREAS, on May 25, 2022, pursuant to Section 2.02 of the Existing Agreement, County exercised its option to extend the term one additional year, effective August 1, 2022 through July 31, 2023; and

WHEREAS, County and Operator now desire to amend the Existing Agreement to extend the term ten (10) additional years for a total investment amount of $1.49 million to improve the Wi-Fi and Distributed Antenna System ("DAS") and $300,000 in additional network upgrades.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, County and Operator hereby agree as follows:

AGREEMENTS

1. **Term of Agreement**. Section 2.01 shall be deleted and replaced with the following:

   "The term of this Agreement shall be extended ten (10) years and shall terminate on July 31, 2033."

2. **Operating Area**. Exhibit A shall be deleted and replaced as attached hereto.

3. **Annual Fee**. Exhibit E shall be deleted and replaced as attached hereto.

4. **Operator's Legal Name**. The Existing Agreement is hereby amended to reflect Operator's true legal name and all references to "Concourse Communications Group" shall be replaced with "Concourse Communications Group, LLC."

5. **Security Plan**. Operator shall establish and maintain a documented cybersecurity program within six (6) months of execution of this First Amendment, to be approved by the Airport Director, addressing all policies, procedures, and technical, physical, and administrative safeguards, as set forth in Exhibit F as applicable, as attached hereto and by this reference made part hereof.

6. **Construction and Installation by Operator.** Sections 7.02(J) and (K) shall be added as follows:

"J. Capital Investment for Wi-Fi and DAS Improvements. OPERATOR shall make a capital investment in the amount of $1.49 million for the following improvements as consideration of this First Amendment:

i. Within one (1) year of execution of this First Amendment, OPERATOR shall upgrade the Wi-Fi system to the new Wi-Fi 6 standard (new Access Points, switches, and associated infrastructure) across the existing coverage areas throughout Terminals A, B, and C, Terminal Administration Office and Badging Office, 3160 Airway Ave, and 3180 Airway Ave.

ii. Within one (1) year of execution of this First Amendment, OPERATOR shall expand the Wi-Fi and DAS coverage area to rideshare pick-up and drop-off areas located in Parking Structure A2, Parking Structure B2, and Parking Structure C, as shown on Exhibit B and approved by the Airport Director. The expansion shall also include the future Customs and Border Protection area and Main Street Parking Lot as needed and approved by the Airport Director

iii. Within three (3) years of execution of this First Amendment, OPERATOR shall complete a full upgrade of the neutral host DAS to 5G for all carriers.

iv. OPERATOR shall continue to upgrade DAS to align with all future iterations of cellular within in one (1) year of general market availability to be aligned with airports of the same size.

K. Additional Upgrades. As consideration of this First Amendment, OPERATOR shall invest a minimum of $300,000 in additional network upgrades, as approved by the Airport Director, over this ten (10) year Agreement extension (August 1, 2023 through July 31, 2033), to address

any performance issues or coverage gaps, support increase demand and speeds and to align with the current technology industry standards. The funds to support this future network upgrade shall not be included in the aforementioned $1.49 million capital investment. Additional network upgrades may be initiated by OPERATOR, upon approval by the Airport Director, based on performance data and technology advances or requests from cellular carriers as their requirements or spectrum evolve."

7. **Nondiscrimination**. Section 11.01 shall be deleted and replaced with the following:

"Section 11.01. NONDISCRIMINATION

A. General Civil Rights Provision

In all its activities within the scope of its airport program, OPERATOR agrees to comply with pertinent statutes, Executive Orders, and such rules as identified in Title VI List of Pertinent Nondiscrimination Acts and Authorities to ensure that no person shall, on the grounds of race, color, national origin (including limited English proficiency), creed, sex (including sexual orientation and gender identity), age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance.

This provision is in addition to that required by Title VI of the Civil Rights Act of 1964.

If the OPERATOR transfers its obligation to another, the transferee is obligated in the same manner as the OPERATOR.

The above provision obligates the OPERATOR for the period during which the property is owned, used or possessed by the OPERATOR and the airport remains obligated to the Federal Aviation Administration.

B. Compliance with Nondiscrimination Requirements

During the performance of this Agreement, OPERATOR, for itself, its personal representatives, successors in interest, and assigns, as a part of the consideration hereof, does hereby covenant and agree as follows:

i. Compliance with Regulations

OPERATOR will comply with the Title VI List of Pertinent Nondiscrimination Acts and Authorities, as they may be amended from time to time, which are herein incorporated by reference and made a part of this Agreement.

ii. Nondiscrimination

OPERATOR, with regard to the work performed by it during the Agreement, will not discriminate on the grounds of race, color, or national origin (including limited English proficiency), creed, sex (including sexual orientation and gender identity), age, or disability, in the selection and retention of subcontractors, including procurement of materials and leases of equipment. OPERATOR will not participate directly or indirectly in the discrimination prohibited by the Nondiscrimination Acts and Authorities, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR part 21.

iii. Solicitations for Subcontracts, including Procurements of Materials and Equipment

In all solicitations, either by competitive bidding or negotiation made by OPERATOR for work to be performed under a subcontract, including procurement of materials, or leases of equipment, each potential subcontractor or supplier will be notified by OPERATOR of the OPERATOR's obligations under this Agreement and the Nondiscrimination Acts and Authorities on the grounds of race, color, or national origin.

iv. Information and Reports

OPERATOR will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the COUNTY or the FAA to be pertinent to ascertain compliance with such Nondiscrimination Acts and Authorities and instructions. Where information required of a contractor is in the exclusive possession of another who fails or refuses to furnish the information, OPERATOR will so certify to the COUNTY or the FAA, as appropriate, and will set forth what efforts it has made to obtain this information.

v. Sanctions for Noncompliance

In the event of the OPERATOR's noncompliance with the non-discrimination provisions of this Agreement, the COUNTY will impose such sanctions as it or the FAA may determine to be appropriate, including, but not limited to: withholding payments under the contract until the OPERATOR complies, and/or cancelling, terminating, or suspending a contract, in whole or in part.

vi. Incorporation of Provisions

The OPERATOR will include the provisions of paragraphs one through six in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations, and directives issued pursuant thereto. The OPERATOR will take action with respect to any sublease, subcontract or procurement as the COUNTY or FAA may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if OPERATOR becomes involved in, or is threatened with litigation by a sub-operator, subcontractor, or supplier because of such direction, the OPERATOR may request the COUNTY to enter into any litigation to protect the interests of the COUNTY. In addition, the OPERATOR may request the United States to enter into the litigation to protect the interests of the United States.

OPERATOR is required to insert the above paragraphs one through six in every sublease or subcontract at any tier. Upon request by the COUNTY, OPERATOR will provide a copy of each sublease or subcontract to demonstrate that the above language has been inserted.

C. Title VI Clauses for Transfer of Real Property and for Construction/Use/Access to Real Property

OPERATOR, for itself, personal representatives, successors in interest, and assigns, as a part of the consideration hereof, does hereby covenant and agree as a covenant running with the land that:

In the event facilities are constructed, maintained or otherwise operated on the Operating Area for a purpose for which a FAA activity, facility, or program is extended or for another purpose involving the provision of similar services or benefits, OPERATOR will maintain and operate such facilities and services in compliance with all requirements imposed by the Nondiscrimination Acts and Regulations listed in the Title VI List of Pertinent Nondiscrimination Acts and Authorities (as may be amended) such that no person on the grounds of race, color, or national origin, will be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination in the use of said facilities.

No person on the ground of race, color, or national origin, will be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination in the use of said facilities.

In the construction of any improvements on, over or under the Operating Area and the furnishing of services thereon, no person on the grounds of race, creed, color, sex, national origin, age, or disability shall be excluded

from participation in, denied the benefits of or otherwise be subjected to discrimination.

OPERATOR will use the Operating Area in compliance with all other requirements imposed by or pursuant to the Title VI List of Pertinent Nondiscrimination Acts and Authorities.

OPERATOR shall furnish its accommodations and/or services on a fair, equal and not unjustly discriminatory basis to all users thereof and it shall charge fair, reasonable and not unjustly discriminatory prices for each unit or service.

D. Title VI List of Pertinent Nondiscrimination Acts and Authorities

During the performance of this contract, OPERATOR, for itself, its assignees, and successors in interest (hereinafter referred to as the "OPERATOR") agrees to comply with the following non-discrimination statutes and authorities; including but not limited to:

i. Title VI of the Civil Rights Act of 1964 (42 USC § 2000d et seq., 78 stat. 252) (prohibits discrimination on the basis of race, color, national origin);

ii. 49 CFR part 21 (Non-discrimination in Federally-Assisted programs of the Department of Transportation—Effectuation of Title VI of the Civil Rights Act of 1964);

iii. The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 USC § 4601) (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);

iv. Section 504 of the Rehabilitation Act of 1973 (29 USC § 794 et seq.), as amended (prohibits discrimination on the basis of disability); and 49 CFR part 27 (Nondiscrimination on the Basis of Disability in Programs or Activities Receiving Federal Financial Assistance);

v. The Age Discrimination Act of 1975, as amended (42 USC § 6101 et seq.) (prohibits discrimination on the basis of age);

vi. Airport and Airway Improvement Act of 1982 (49 USC § 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex);

vii. The Civil Rights Restoration Act of 1987 (PL 100-259) (broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, the Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, sub-recipients and contractors, whether such programs or activities are Federally funded or not);

viii. Titles II and III of the Americans with Disabilities Act of 1990 (42 USC § 12101, et seq) (prohibit discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities) as implemented by U.S. Department of Transportation regulations at 49 CFR parts 37 and 38;

ix. The Federal Aviation Administration's Nondiscrimination statute (49 USC § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);

x. Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations (ensures nondiscrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations);

xi. Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs [70 Fed. Reg. 74087 (2005)];

xii. Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 USC § 1681, et seq).

OPERATOR is required to insert the above Title VI List of Pertinent Nondiscrimination Acts and Authorities into every sublease or subcontract at any tier. Upon request by the COUNTY, OPERATOR will provide a copy of each sublease or subcontract to demonstrate that the above language has been inserted."

8. **ACDBE Participation**. Section 11.09 shall be added as follows:

"Section 11.09 AIRPORT CONCESSION DISADVANTAGED BUSINESS ENTERPRISE (ACDBE) PARTICIPATION

A. ACDBE Program Assurances

This Agreement is subject to the requirements of the U.S. Department of Transportation's regulations at 49 CFR Part 23. OPERATOR agrees that it will not discriminate against any business owner because of the owner's race, color, national origin, or sex in connection with the award or performance of any concession agreement, management contract or subcontract, purchase or lease agreement covered by 49 CFR Part 23.

OPERATOR agrees to include the above statements in any subsequent agreement or contract covered by 49 CFR part 23 that it enters and cause those businesses to similarly include such statements in further agreements.

B. ACDBE Termination or Substitution

If OPERATOR proposes to terminate, substitute, or modify the participation of an ACDBE Joint Venture partner, team member, subcontractor, or sub-concessionaire in the Agreement before or after Agreement award, prior to such change, the OPERATOR shall immediately submit for review to the Airport's ACDBE Liaison Officer an explanation and reasonable documentation regarding the proposed change in ACDBE participation. OPERATOR shall include the specific reasons for the change in ACDBE participation and must produce any requested documents and information regarding the proposed change.

C. Monitoring and Reporting Requirements

OPERATOR agrees to submit any report(s) or information that COUNTY is required by law or regulation to obtain from OPERATOR, or which the Airport's ACDBE Liaison Officer or designee may request relating to OPERATOR's operations. In addition, OPERATOR shall provide all information and reports required by the Airport and shall permit access to its books, records, accounts, other sources of information and its facilities as may be determined by the Airport to be pertinent to ascertain compliance with the regulations or directives.

OPERATOR shall timely submit reports and verifications requested by the COUNTY and shall provide such financial information or other information deemed necessary by it to support and document the ACDBE participation for this Agreement. COUNTY shall have the right until six (6) years after the expiration or termination of this Agreement, through its representatives, and at all reasonable times, to review books, records, and financial information of the OPERATOR (and where applicable, all individuals, Joint Venture partners or team members or other business entities that are a party or engaged in concession activity under this Agreement) requested by representatives of the COUNTY to substantiate compliance with 49 CFR Parts 23 and 26 as amended, and any guidance issued by FAA regarding the interpretation of the federal regulations.

D. Other Requirements

OPERATOR shall comply with the requirements of 49 CFR Part 23 and 26, the Airport's ACDBE Program, and guidance issued by the FAA, regarding the interpretation of the regulations, including but not limited to the Joint Venture Guidance in the administration of this Agreement. OPERATOR shall comply with any future amendments to the aforementioned authorities.

E. Non-Compliance

In the event of OPERATOR's non-compliance with the ACDBE Program, COUNTY may, in addition to pursuing any other available legal remedy, terminate, suspend or cancel this Agreement in whole or in part; and/or suspend or debar OPERATOR from eligibility to contract with COUNTY in the future or to receive bid packages or request for proposal packages or other solicitations, unless OPERATOR demonstrates, within a reasonable time as determined by COUNTY, its compliance with the terms of the ACDBE Program or this Article."

9. No Other Amendments; This First Amendment Governs and Controls. Except as expressly modified by this First Amendment, the Existing Agreement shall remain unmodified and in full force and effect and is hereby reinstated, ratified, and affirmed. To the extent any of the provisions of this First Amendment are inconsistent with any of the provisions set forth in the Existing Agreement, the provisions of this First Amendment shall govern and control. Any reference to the "Agreement," "hereunder," "hereof," "herein," or words of like import in the Existing Agreement and this First Amendment shall mean and be a reference to the Existing Agreement as hereby amended, and the Existing Agreement and this First Amendment shall be read and interpreted as if it was one Agreement.

10. Authority. Each Party represents to the other Party or Parties that the individual executing this First Amendment on behalf of such Party has the capacity and authority to execute and deliver this First Amendment on behalf of such Party, and that this First Amendment, once executed and delivered, is the legal, valid, and binding obligation of such Party.

11. **Governing Law**. This First Amendment, and the Existing Amendment, shall be governed by and construed in accordance with the laws of the State of California.

12. **Counterparts and Execution**. This First Amendment may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same document. The delivery of an executed counterpart of this First Amendment by facsimile or as a Portable Document Format ("PDF") or similar attachment to an e-mail shall constitute effective delivery of such counterpart for all purposes with the same force and effect as the delivery of an original, executed counterpart.

13. **Severability**. If any provision of this First Amendment is determined by a court of competent jurisdiction to be invalid or unenforceable, the remainder of this First Amendment shall nonetheless remain in full force and effect.

14. **Contractual Obligation**. Operator shall be current on all contractual obligations, including but not limited to, monthly fees, Insurance, Security Deposit, late fees, penalties, and fines through June 30, 2023, except as otherwise provided for herein. Operator shall maintain JWA-approved locations within the Operating Area.

[*Signatures appear on the following page*]

IN WITNESS WHEREOF, the Parties have executed this Amendment the day and year first above written.

OPERATOR: Concourse Communications Group, LLC.

DocuSigned by:
By: _____ B35360E41BA041B...
Its: CFO
Name: Peter Hovenier

By: _____
Its: _____
Name: _____

APPROVED AS TO FORM:
County Counsel
DocuSigned by:
By: Mark Sanchez 5EE66EC8DA7B48F...

APPROVED AS TO AUDIT AND ACCOUNTING:
Auditor-Controller
DocuSigned by:
By: Katherine Buranday 996FC039E3774ED...

RECOMMENDED FOR APPROVAL:
John Wayne Airport
DocuSigned by:
By: Charlene Reynolds A1A526A921AF49F...
Charlene Reynolds
Airport Director

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIR OF THE BOARD PER G.C. SEC. 25103, RESO 79-1535
ATTEST:

Clerk of the Board of Supervisors
Orange County, California

COUNTY

COUNTY OF ORANGE

By: _____
Chairman, Board of Supervisors

EXHIBIT A

OPERATING AREA

EXHIBIT A - OPERATING AREA

Access Points Report

Project name:	SNA 2023	**Design company:**	
Project creation date:	4/6/2023	**Designer:**	

3160 Airport Ave: 3160

EXHIBIT A

	ID	Model
1	AP6001	C9130AXI-EWC-x
2	AP6002	C9130AXI-EWC-x
3	AP6003	C9130AXI-EWC-x
4	AP6004	C9130AXI-EWC-x
5	AP6005	C9130AXI-EWC-x
6	AP6006	C9130AXI-EWC-x
7	AP6007	C9130AXI-EWC-x
8	AP6008	C9130AXI-EWC-x
9	AP6009	C9130AXI-EWC-x
10	AP6010	C9130AXI-EWC-x
11	AP6011	C9130AXI-EWC-x
12	AP6012	C9130AXI-EWC-x
13	AP6013	C9130AXI-EWC-x
14	AP6014	C9130AXI-EWC-x
15	AP6015	C9130AXI-EWC-x
16	AP6016	C9130AXI-EWC-x
17	AP6017	C9130AXI-EWC-x

17	AP6017	C9130AXI-EWC-x
18	AP6018	C9130AXI-EWC-x
19	AP6019	C9130AXI-EWC-x
20	AP6020	C9130AXI-EWC-x
21	AP6021	C9130AXI-EWC-x
22	AP6022	C9130AXI-EWC-x
23	AP6023	C9130AXI-EWC-x
24	AP6024	C9130AXI-EWC-x
25	AP6025	C9130AXI-EWC-x
26	AP6026	C9130AXI-EWC-x

Access Points Report

Project name:	SNA 2023	**Design company:**	
Project creation date:	4/6/2023	**Designer:**	

Building 1: Terminal A & B - Arrival Level

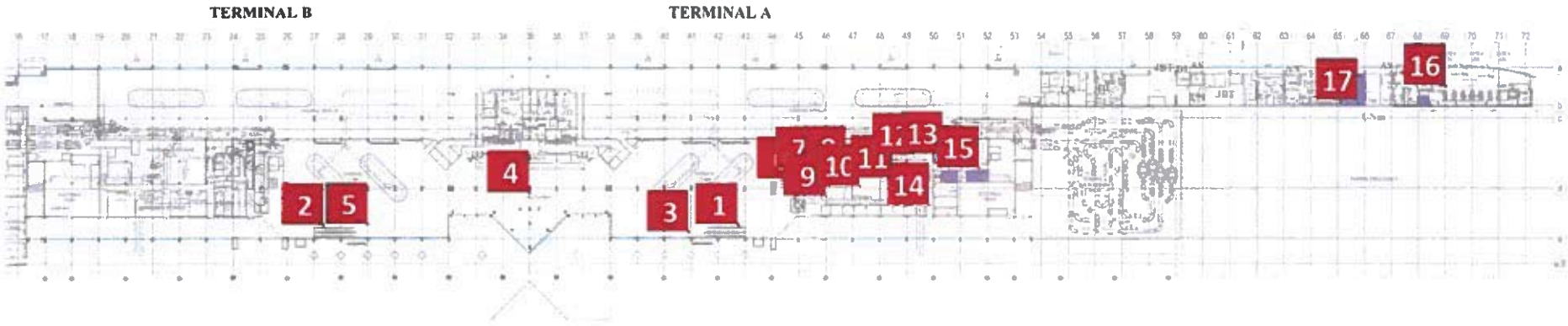
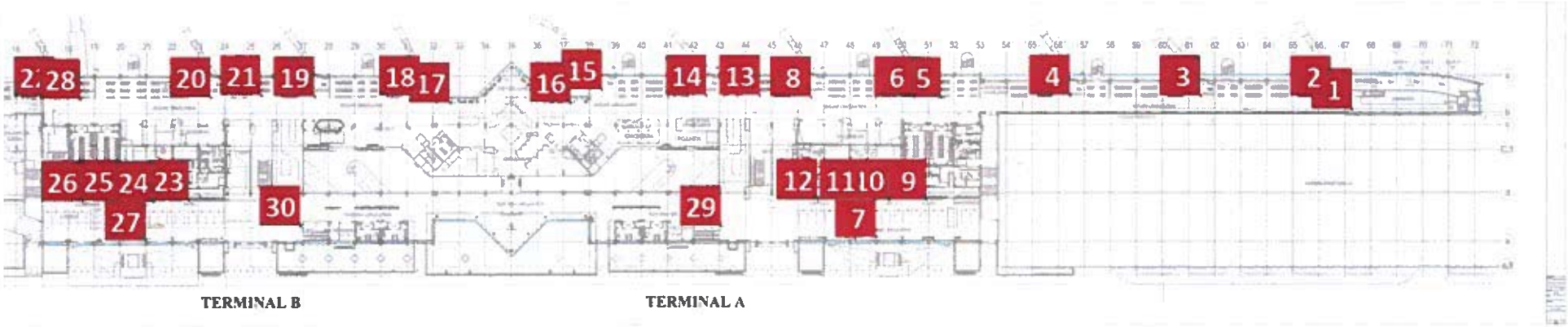


EXHIBIT A

	ID	Model
1	AP1001	C9130AXE-EWC-x
2	AP1005	C9130AXE-EWC-x
3	AP1006	C9130AXI-EWC-x
4	AP1007	C9130AXI-EWC-x
5	AP1008	C9130AXI-EWC-x
6	AP1009	C9130AXI-EWC-x
7	AP1010	C9130AXI-EWC-x
8	AP1011	C9130AXI-EWC-x
9	AP1012	C9130AXI-EWC-x
10	AP1013	C9130AXI-EWC-x
11	AP1014	C9130AXI-EWC-x
12	AP1015	C9130AXI-EWC-x
13	AP1016	C9130AXI-EWC-x
14	AP1017	C9130AXI-EWC-x
15	AP1018	C9130AXI-EWC-x
16	AP1019	C9130AXI-EWC-x
17	AP1020	C9130AXI-EWC-x

17	AP1020	C9130AXI-EWC-x

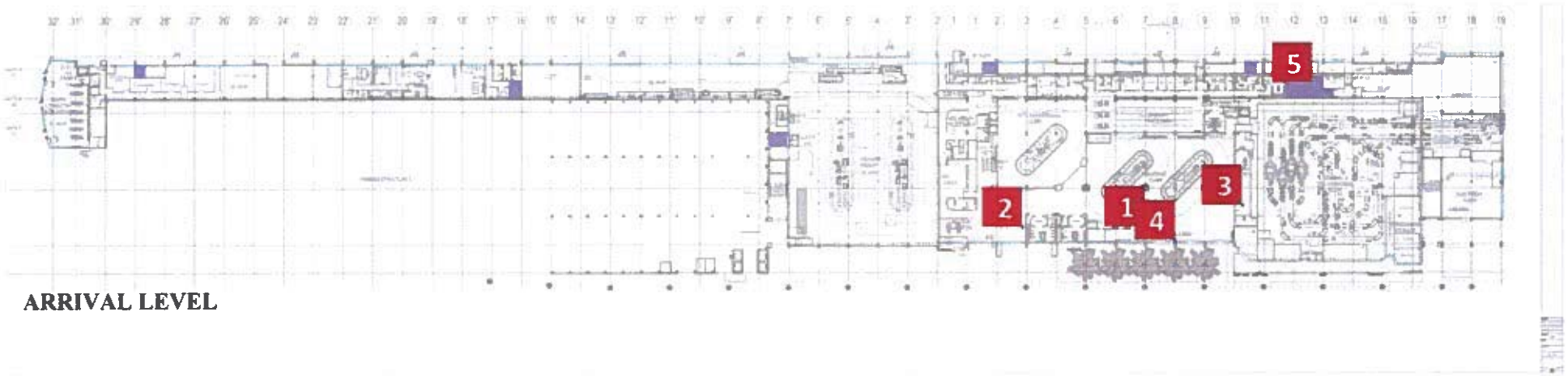
Building 1: Terminal A & B - Departure Level



	ID	Model
1	AP2002	C9130AXE-EWC-x
2	AP2003	C9130AXE-EWC-x
3	AP2004	C9130AXE-EWC-x
4	AP2006	C9130AXE-EWC-x
5	AP2007	C9130AXE-EWC-x
6	AP2008	C9130AXE-EWC-x
7	AP2009	C9130AXE-EWC-x
8	AP2010	C9130AXE-EWC-x
9	AP2013	C9130AXI-EWC-x
10	AP2014	C9130AXI-EWC-x
11	AP2015	C9130AXI-EWC-x
12	AP2016	C9130AXI-EWC-x
13	AP2017	C9130AXE-EWC-x
14	AP2018	C9130AXE-EWC-x
15	AP2019	C9130AXE-EWC-x
16	AP2020	C9130AXE-EWC-x
17	AP2021	C9130AXE-EWC-x

17	AP2021	C9130AXE-EWC-x
18	AP2022	C9130AXE-EWC-x
19	AP2023	C9130AXE-EWC-x
20	AP2024	C9130AXE-EWC-x
21	AP2025	C9130AXE-EWC-x
22	AP2026	C9130AXE-EWC-x
23	AP2027	C9130AXI-EWC-x
24	AP2028	C9130AXI-EWC-x
25	AP2029	C9130AXI-EWC-x
26	AP2030	C9130AXI-EWC-x
27	AP2031	C9130AXE-EWC-x
28	AP2032	C9130AXE-EWC-x
29	AP2033	C9130AXE-EWC-x
30	AP2034	C9130AXE-EWC-x

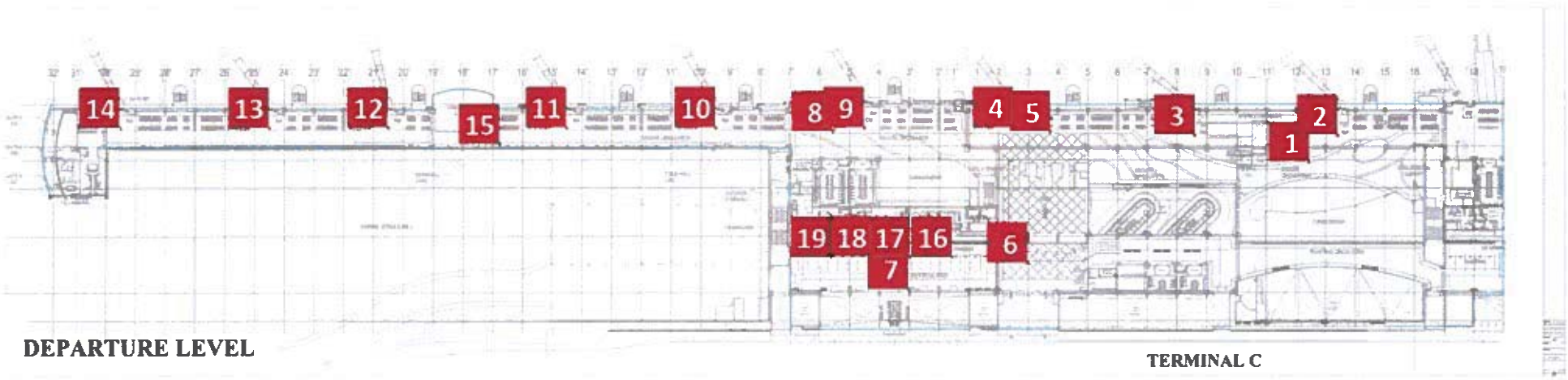
Building 1: Terminal C - Arrival Level



ARRIVAL LEVEL

	ID	Model
1	AP3001	C9130AXE-EWC-x
2	AP3003	C9130AXE-EWC-x
3	AP3004	C9130AXI-EWC-x
4	AP3005	C9130AXE-EWC-x
5	AP3006	C9130AXI-EWC-x

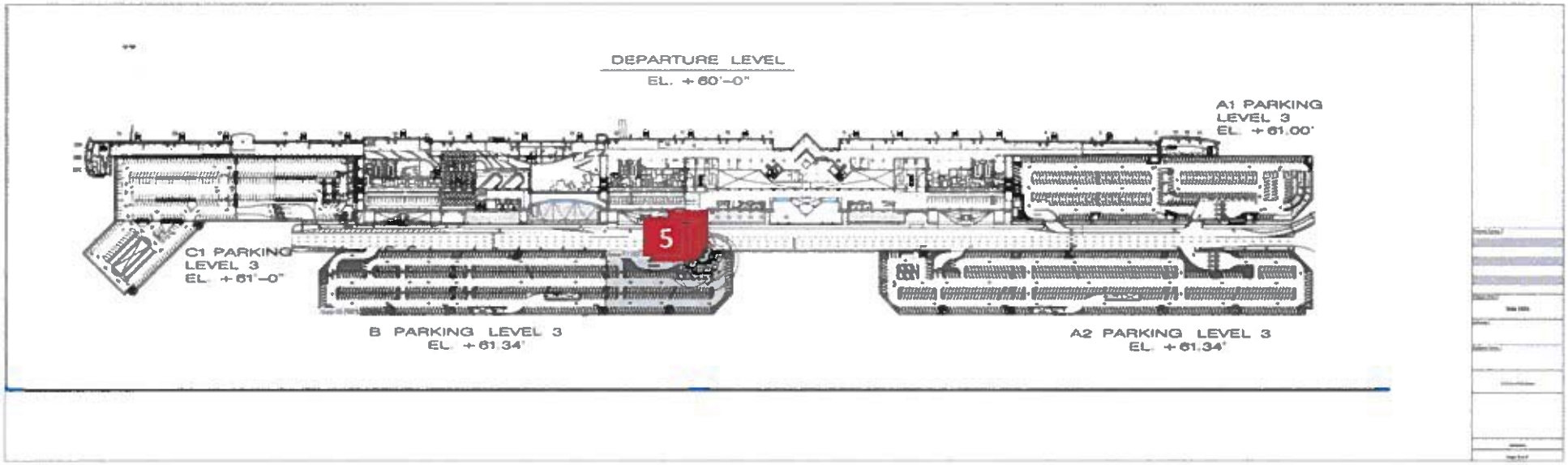
Building 1: Terminal C - Departure Level



	ID	Model
1	AP4001	C9130AXE-EWC-x
2	AP4002	C9130AXE-EWC-x
3	AP4003	C9130AXE-EWC-x
4	AP4004	C9130AXE-EWC-x
5	AP4005	C9130AXE-EWC-x
6	AP4006	C9130AXE-EWC-x
7	AP4007	C9130AXE-EWC-x
8	AP4008	C9130AXE-EWC-x
9	AP4009	C9130AXE-EWC-x
10	AP4010	C9130AXE-EWC-x
11	AP4011	C9130AXE-EWC-x
12	AP4012	C9130AXE-EWC-x
13	AP4013	C9130AXE-EWC-x
14	AP4014	C9130AXE-EWC-x
15	AP4015	C9130AXE-EWC-x
16	AP4017	C9130AXI-EWC-x
17	AP4018	C9130AXI-EWC-x

17	AP4018	C9130AXI-EWC-x
18	AP4019	C9130AXI-EWC-x
19	AP4020	C9130AXI-EWC-x

Building 1: 3rd Level Rideshare



	ID	Model
1	AP5001	C9124AXI
2	AP5002	C9124AXI
3	AP5003	C9124AXI
4	AP5004	C9124AXI
5	AP5005	C9124AXI

Access Points Report

Project name:	SNA 2023	**Design company:**	
Project creation date:	4/6/2023	**Designer:**	

3180 Airport Ave: 3180

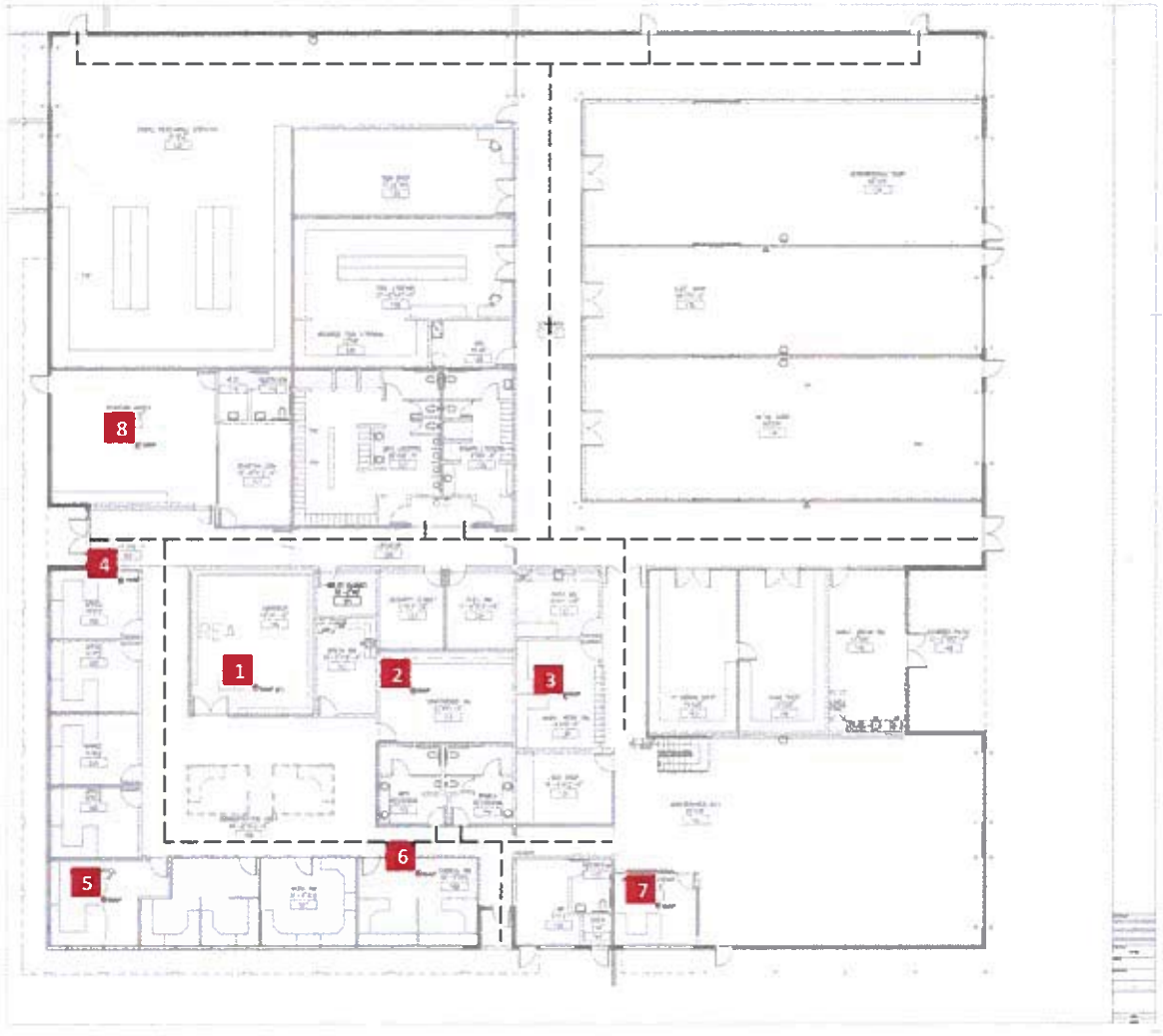


EXHIBIT A

Attachment A

	ID	Model
1	AP7001	C9130AXI-EWC-x
2	AP7002	C9130AXI-EWC-x
3	AP7003	C9130AXI-EWC-x
4	AP7004	C9130AXI-EWC-x
5	AP7005	C9130AXI-EWC-x
6	AP7006	C9130AXI-EWC-x
7	AP7007	C9130AXI-EWC-x
8	AP7008	C9130AXI-EWC-x

EXHIBIT E
SPECIAL PROVISIONS

SECTION 4.01 FEE

OPERATOR agrees to pay the following fees, payable monthly in arrears, on or before the twentieth day of each month.

Annual Fee. OPERATOR shall pay to COUNTY for each accounting year the Annual Fee based on the following schedule:

Year One (1) 2014 – 2015	$150,000	One Hundred and Fifty Thousand Dollars
Year Two (2) 2015 – 2016	$150,000	One Hundred and Fifty Thousand Dollars
Year Three (3) 2016 – 2017	$150,000	One Hundred and Fifty Thousand Dollars
Year Four (4) 2017 – 2018	$150,000	One Hundred and Fifty Thousand Dollars
Year Five (5) 2018 – 2019	$150,000	One Hundred and Fifty Thousand Dollars
Year Six (6) 2019 – 2020	$150,000	One Hundred and Fifty Thousand Dollars
Year Seven (7) 2020 – 2021	$150,000	One Hundred and Fifty Thousand Dollars
Year Eight (8) 2021 – 2022	$150,000	One Hundred and Fifty Thousand Dollars
Year Nine (9) 2022 – 2023	$150,000	One Hundred and Fifty Thousand Dollars
Year Ten (10) 2023 – 2024	$150,000	One Hundred and Fifty Thousand Dollars
Year Eleven (11) 2024 – 2025	$150,000	One Hundred and Fifty Thousand Dollars
Year Twelve (12) 2025 – 2026	$150,000	One Hundred and Fifty Thousand Dollars
Year Thirteen (13) 2026 – 2027	$150,000	One Hundred and Fifty Thousand Dollars
Year Fourteen (14) 2027 – 2028	$150,000	One Hundred and Fifty Thousand Dollars
Year Fifteen (15) 2028 – 2029	$150,000	One Hundred and Fifty Thousand Dollars
Year Sixteen (16) 2029 – 2030	$150,000	One Hundred and Fifty Thousand Dollars
Year Seventeen (17) 2030 – 2031	$150,000	One Hundred and Fifty Thousand Dollars
Year Eighteen (18) 2031 – 2032	$150,000	One Hundred and Fifty Thousand Dollars
Year Nineteen (19) 2032 – 2033	$150,000	One Hundred and Fifty Thousand Dollars

EXHIBIT F

COUNTY OF ORANGE INFORMATION TECHNOLOGY STANDARDS

EXHIBIT F

County of Orange

Information Technology Security Standards

1 ASSET MANAGEMENT

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that shall allow the assets to maintain productivity during disruptive events. There are four broad categories of assets: people, information, technology, and facilities.

The Cybersecurity Program strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data.

1.1 GOALS AND OBJECTIVES

1.1.1 Services are identified and prioritized.

1.1.2 Assets are inventoried, and the authority and responsibility for these assets is established.

1.1.3 The relationship between assets and the services they support is established.

1.1.4 The asset inventory is managed.

1.1.5 Access to assets is managed.

1.1.6 Information assets are categorized and managed to ensure the sustainment and protection of the critical service.

1.1.7 Facility assets supporting the critical service are prioritized and managed.

1.2 ASSET MANAGEMENT POLICY STATEMENTS

1.2.1 Services Inventory

1.2.1.1 Departments shall maintain an inventory of its services. This listing shall be used by the department to assist with its risk management analysis.

1.2.2 Asset Inventory – Information

1.2.2.1 All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property shall be used in compliance with this policy.

1.2.2.2 County information is a valuable asset and shall be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices shall be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.

1.2.2.3 Departments shall establish internal procedures for the secure handling and storage of all electronically-maintained County information that is owned or controlled by the department.

1.2.3 Asset Inventory - Technology (Devices, Software)

1.2.3.1 Departments shall maintain an inventory of all department managed devices that connect to County network resources or processes, stores, or transmits County data including but not limited to:

- Desktop computers,
- Laptop Computers,
- Tablets (iPads and Android devices),
- Mobile Phones (basic cell phones),
- Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),
- Servers,
- Storage devices,
- Network switches,
- Routers,
- Firewalls,
- Security Appliances,
- Internet of Things (IoT) devices,
- Printers,
- Scanners,
- Kiosks and Thin clients,
- Mainframe Hardware, and
- VoIP Phones.

1.2.3.2 Asset inventory shall map assets to the services they support.

1.2.3.3 Departments shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased) that, at a minimum, includes the following:

- Department (see Appendix A for an example Department Listing)
- Facility (see Appendix B for an example Facility Listing)
- Device Type (see Appendix C for an example Device Type Listing)

1.2.3.4 Each department shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.

1.2.4 Asset Inventory - Facilities

1.2.4.1 Departments shall maintain an inventory of its facilities. This listing shall be used by the department to assist with its risk management analysis.

1.2.4.2 Departments shall identify the facilities used by its critical services.

1.2.5 Access Controls

Refer to *User Provisioning Policy* for additional guidance.

1.2.5.1 Departments shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

1.2.5.2 Access to County information systems and information systems data shall be based on each user's access privileges. Access controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle.

1.2.5.3 Access to County information and County information assets should be based on the principle

of "least privilege," that is, grant no user greater access privileges to the information or assets than County responsibilities demand.

1.2.5.4 The owner of each County system, or their designee, provides written authorization for all internal and external user access.

1.2.5.5 All access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier (ID) and password combination that provides verification of the user's identity.

1.2.5.6 All County workforce members are to be assigned a unique user ID to access the network.

1.2.5.7 A user account shall be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need shall be documented prior to account creation and accounts activated only when necessary.

1.2.5.8 User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.

1.2.5.9 Departments shall conduct regular reviews of the registered users' access level privileges. System owners shall provide user listings to departments for confirmation of user's access privileges.

1.2.6 Asset Sanitation/Disposal

1.2.6.1 Unless approved by County management, no County computer equipment shall be removed from the premises.

1.2.6.2 Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.

1.2.6.3 Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.

1.2.6.4 Sanitization methods for media containing County information shall be in accordance with NSA standards (for example, clearing, purging, or destroying).

1.2.6.5 Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

2 CONTROLS MANAGEMENT

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. This process helps the organization ensure the controls management objectives are satisfied.

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess.

2.1 GOALS AND OBJECTIVES

2.1.1 Control objectives are established.

2.1.2 Controls are implemented.

2.1.3 Control designs are analyzed to ensure they satisfy control objectives.

2.1.4 Internal control system is assessed to ensure control objectives are met.

2.2 CONTROL MANAGEMENT POLICY STATEMENTS

2.2.1 Physical and Environmental Security

2.2.1.1 Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.

2.2.1.2 Restricted areas within facilities that house sensitive or critical County information systems shall, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

2.2.1.3 Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.

2.2.1.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.

2.2.1.5 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.

2.2.1.6 Continuity of power shall be provided to maintain the availability of critical equipment and information systems.

2.2.1.7 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Different, yet appropriate methods shall be utilized for internal and external cabling.

2.2.1.8 Equipment shall be properly maintained to ensure its continued availability and integrity.

2.2.1.9 All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.

2.2.2 Network Segmentation

NOTE: This section is applicable to Departments that manage their own network devices.

2.2.2.1 Segment (e.g., VLANs) the network into multiple, separate zones (based on trust levels of the information stored/transmitted) to provide more granular control of system access and additional intranet boundary defenses. Whenever information flows over a network of lower trust level, the information shall be encrypted.

2.2.2.2 Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.

2.2.2.3 Create separate network segments (e.g., VLANs) for BYOD (bring your own device) systems or other untrusted devices.

2.2.2.4 The network infrastructure shall be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

2.2.3 Mobile Computing Devices

To ensure that Mobile Computing Devices (MCDs) do not introduce threats into systems that process or store County information, departments' management shall:

2.2.3.1 Establish and manage a process for authorizing, issuing and tracking the use of MCDs.

2.2.3.2 Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.

2.2.3.3 Implement applicable access control requirements in accordance with this policy, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.

2.2.3.4 Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information. See Section on Encryption.

2.2.3.5 Ensure that MCDs are configured to restrict the user from circumventing the authentication process.

2.2.3.6 Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.

2.2.3.7 Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.

2.2.3.8 The installation of any software, executable, or other file to any County computing device is prohibited if that software, executable, or other file downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds unless approved by the department. If the device ("i" device or smartphone, only) complies with the mobile device management security standards (see section 9.2.3 Mobile Computing Devices), this is not applicable.

2.2.4 Personally Owned Devices

Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (PDA's) owned by or purchased by employees, contract personnel, or other non-County users.

2.2.4.1 The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless previously

approved.

2.2.4.2 The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County's Microsoft Office 365 environment, OC Expediter, and VTI timesheet applications, to name a few. Access to some agency specific applications, e.g. applications that are subject to compliance regulations may require prior approval of the County CISO and the associated Department Head.

2.2.4.3 The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources.

2.2.4.4 The County will only request access to the personally owned device in order to implement security controls; to respond to litigation hold (aka: e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized technician or designee using a legitimate software process.

2.2.5 Logon Banners and Warning Notices

2.2.5.1 At the time of network login, the user shall be presented with a login banner.

2.2.5.2 All computer systems that contain or access County information shall display warning banners informing potential users of conditions of use consistent with state and federal laws.

2.2.5.3 Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.

2.2.5.4 The banner message shall be placed at the user authentication point for every computer system that contains or accesses County information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

2.2.5.5 At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:

- User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

2.2.6 Authentication

2.2.6.1 Authenticate user identities at initial connection to County resources.

2.2.6.2 Authentication mechanisms shall be appropriate to the sensitivity of the information contained.

2.2.6.3 Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

2.2.7 Passwords

2.2.7.1 County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices (see Section 9.2.4 Mobile Computing Devices for additional guidance on mobile devices) and personally owned devices used for work (see Section 9.2.5 Personally Owned Devices for additional guidance on personally owned devices).

2.2.7.2 Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:

- Passwords will contain a minimum of one upper case letter
- Passwords will contain a minimum of one lower case letter
- Passwords will contain a minimum of one number: 1- 0
- Passwords will contain a minimum of one symbol: !,@,#,$,%,^,&,*,(,)
- Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
- Passwords characters will not be repeated in a row (Do not use: P@$$S. This is ok: P@S)
- COMPLEX PASSWORD EXAMPLE: P@$SWoRd13

2.2.7.3 Passwords shall have a minimum length of 8 characters.

2.2.7.4 Passwords shall not be reused for twelve iterations.

2.2.7.5 Departments shall require users to change their passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

2.2.7.6 Network and application systems shall be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum) when the technology is feasible or available.

2.2.7.7 Newly-created accounts shall be assigned a randomly generated password prior to account information being provided to the user.

2.2.7.8 No user shall give his or her password to another person under any circumstances. Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management in accordance with Section 12: Incident Management.

2.2.7.9 Users who have lost or forgotten their passwords shall make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester shall be authenticated to the user account in question. (e.g., Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords shall be provided directly and only to the user in question.

2.2.7.10 When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

2.2.7.11 All passwords are to be treated as sensitive information.

2.2.7.12 User Accounts shall be locked after five consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID after investigation. These features shall be configured as indicated when the technology is feasible or available.

2.2.7.13 All systems containing sensitive information shall not allow users to have multiple concurrent sessions on the same system when the technology is feasible or available.

2.2.8 Inactivity Timeout and Restricted Connection Times

2.2.8.1 Automatic lockouts for system devices, including workstations and mobile computing devices (refer to Section 9.2.4 Mobile Computing Devices), after no more than 15 minutes of inactivity.

2.2.8.2 Automated screen lockouts shall be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures shall be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members shall not leave their computer unattended or available for someone else to use.

2.2.8.3 When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections shall be accepted.

2.2.9 Account Monitoring

2.2.9.1 Access to a County network and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These shall be secured to ensure County resources are not accessed by unauthorized users.)

2.2.9.2 The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.

2.2.9.3 Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.

2.2.9.4 After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.

2.2.9.5 On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

2.2.10 Administrative Privileges

2.2.10.1 Systems Administrators shall use separate administrative accounts, which are different from their end user account (required to have an individual end user account), to conduct system administration tasks.

2.2.10.2 Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.

2.2.10.3 Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative (e.g., DISO) using the Security Review and Approval Process.

2.2.10.4 Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the Security Review and Approval Process.

2.2.10.5 Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.

2.2.10.6 All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Section 9.2.8.

2.2.11 Remote Access

2.2.11.1 Departments shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.

2.2.11.2 Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.

2.2.11.3 All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by OCIT Enterprise Privacy and Cybersecurity. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.

2.2.11.4 Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.

2.2.11.5 All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.

2.2.11.6 All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.

2.2.11.7 Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.

2.2.11.8 Users granted remote access to County IT infrastructure shall follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.

2.2.11.9 Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.

2.2.11.10 All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department DISO and OCIT Enterprise Privacy and Cybersecurity. This approval shall be received prior to the start of such implementation. The approval shall be developed as a memorandum of understanding (MOU).

2.2.11.11 Remote access privileges to County IT resources shall not be given to contractors, customers or vendors unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.

2.2.12 Wireless Access

2.2.12.1 Departments shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.

2.2.12.2 Only wireless systems that have been evaluated for security by both department management and OCIT Enterprise Privacy and Cybersecurity shall be approved for connectivity to County networks.

2.2.12.3 County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.

2.2.12.4 All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, vendors and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.

2.2.12.5 Each department shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

2.2.13 System and Network Operations Management

2.2.13.1 Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.

2.2.13.2 Departments shall establish controls to ensure the security of the information systems networks that they operate.

2.2.13.3 Operational system documentation for County information systems shall be protected from unauthorized access.

2.2.13.4 System utilities shall be available to only those users who have a business case for accessing the specific utility.

2.2.14 System Monitoring and Logging

2.2.14.1 Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.

2.2.14.2 Each department shall maintain a log of all faults involving County information systems and services.

2.2.14.3 Logs shall be protected from unauthorized access or modifications wherever they reside.

2.2.14.4 The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.

2.2.14.5 Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.

2.2.14.6 Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

2.2.15 Malware Defenses

2.2.15.1 Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti-spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and white listing and black listing of applications, web sites, and IP addresses.

2.2.15.2 Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.

2.2.15.3 Where feasible, any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network shall be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

2.2.16 Data Loss Prevention

2.2.16.1 Departments shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.

2.2.16.2 Departments shall deploy encryption software on mobile devices containing sensitive. See Section 9.2.19 Encryption for additional guidance.

2.2.17 Data Transfer

2.2.17.1 Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.

2.2.17.2 County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

2.2.18 Encryption

2.2.18.1 The decision to use cryptographic controls and/or data encryption in an application shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.2 The decision to use cryptographic controls and/or data encryption on a hard drive shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.3 Where appropriate, encryption shall be used to protect confidential (as defined by County policy) application data that is transmitted over open, untrusted networks, such as the Internet.

2.2.18.4 When cryptographic controls are used, procedures addressing the following areas shall be established by each department:

- Determination of the level of cryptographic controls
- Key management/distribution steps and responsibilities

2.2.18.5 Encryption keys shall be exchanged only using secure methods of communication.

2.2.19 System Acquisition and Development

2.2.19.1 Departments shall identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the department as well as other business applications that are used by the department but owned and/or managed by other County organizations. All business applications used by a department shall be documented in the department's IT security plan as well as their Business Impact Analysis (BIA).

2.2.19.2 An application owner shall be designated for each internal department business application.

2.2.19.3 All access controls associated with business applications shall be commensurate with the highest level of data used within the application. These same access controls shall also adhere to the policy provided in Section 7: Access Control.

2.2.19.4 Security requirements shall be incorporated into the evaluation process for all commercial software products that are intended to be used as the basis for a business application. The security requirements in question shall be based on requirements and standards specified in this policy.

2.2.19.5 In situations where data needs to be isolated because there would be a conflict of interest (e.g., DA and OCPD data cannot be shared), data security shall be designed and implemented to ensure that isolation.

Business Requirements

2.2.19.6 The business requirements definition phase of system development shall contain a review to ensure that the system shall adhere to County information security standards.

System Files

2.2.19.7 Operating system files, application software and data shall be secured from unauthorized use or access.

2.2.19.8 Clear-text data that results from testing shall be handled, stored, and disposed of in the same

manner and using the same procedures as are used for production data.

2.2.19.9 System tests shall be performed on data that is constructed specifically for that purpose.

2.2.19.10 System testing shall not be performed on operational data unless the necessary safeguards are in place.

2.2.19.11 A combination of technical, procedural and physical safeguards shall be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

System Development & Maintenance

2.2.19.12 The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.

2.2.19.13 When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade shall be completed in advance in order to minimize potential security risks and disruptions to the production environment.

2.2.19.14 Any outside suppliers used for maintenance that are visitors to the facility are to be escorted and monitored while performing maintenance to critical systems. This does not apply to contractors that are assigned to work at the facility.

2.2.19.15 Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.

2.2.19.16 All County workforce members shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.

2.2.19.17 In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.

2.2.19.18 Departments are responsible for managing outsourced software development related to department-owned IT systems.

System Requirements

Any system that processes or stores County Information shall:

2.2.19.19 Baseline configuration shall incorporate Principle of Least Privilege and Functionality.

2.2.19.20 Systems shall be deployed where feasible to utilize existing County authentication methods.

2.2.19.21 Session inactivity timeouts shall be implemented for all access into and from County networks.

2.2.19.22 All applications are to have access controls unless specifically designated as a public access resource.

2.2.19.23 Meet the password requirements defined in Section 9.2.8: Passwords.

2.2.19.24 Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.

2.2.19.25 Monitor special privilege access, e.g. administration accounts.

2.2.19.26 Restrict authority to change master files to persons independent of the data processing function.

2.2.19.27 Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.

2.2.19.28 Be capable of routinely monitoring the access to automated systems containing County Information.

2.2.19.29 Log all modifications to the system files.

2.2.19.30 Limit access to system utility programs to necessary individuals with specific designation.

2.2.19.31 Maintain audit logs on a device separate from the system being monitored.

2.2.19.32 Delete or disable all default accounts.

2.2.19.33 Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes shall be applied only through the appropriate change control process.

2.2.19.34 Restrict access to server-file-system controls that allow access to other users' files.

2.2.19.35 Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

2.2.20 Procurement Controls

2.2.20.1 Breach notification requirements clause to be included in new or renewal contracts (once policy is effective) for systems containing sensitive information.

> Contractor shall report to the County within 24 hours as defined in this contract when Contractor becomes aware of any suspected data breach of Contractor's or Sub-Contractor's systems involving County's data.

2.2.20.2 Departments shall review all procurements and renewals for software and equipment (hosted/managed by the vendor) that transmits, stores, or processes sensitive information to ensure that vendors and contractors are aware of and are in compliance with County's cybersecurity policies. Departments shall obtain documentation supporting the business partners, contractors, consultants, or vendors compliance with County's cybersecurity policies such as:

- SOC 1 Type 2
- SOC 2 Type 2
- Security Certifications (ISO, PCI, etc.)
- Penetration Test Results

2.2.21 IT Services Provided to Public

2.2.21.1 Public access to County electronic information resources shall provide desired services in accordance with safeguards designed to protect County resources. All County electronic information resources are to be reviewed at least quarterly.

2.2.22 Removable Media

2.2.22.1 When no longer required, the contents of removable media shall be permanently destroyed or rendered unrecoverable in accordance with applicable department, County, state, or federal record disposal and/or retention requirement

3 CONFIGURATION & CHANGE MANAGEMENT

Configuration and Change Management (CCM) is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

Cybersecurity is an integral component to information systems from the onset of the project or acquisition through implementation of:

- Application and system security
- Configuration management
- Change control procedures
- Encryption and key management
- Software maintenance, including but not limited to, upgrades, antivirus, patching and malware detection response systems

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization.

3.1 GOALS AND OBJECTIVES

3.1.1 The lifecycle of assets is managed.

3.1.2 The integrity of technology and information assets is managed.

3.1.3 Asset configuration baselines are established.

3.2 CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

3.2.1 Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.

3.2.2 Changes impacting security appliances managed by OCIT (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by OCIT Enterprise Privacy and Cybersecurity in accordance with the County Security Review and Approval Process.

3.2.3 Only authorized users shall make any changes to system and/or software configuration files.

3.2.4 Only authorized users shall download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems without prior written authorization from department IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.

3.2.5 Each department shall develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.

3.2.6 Each department shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.

3.2.7 As appropriate, segregation of duties shall be implemented by all County departments to ensure that no single person has control of multiple critical systems and the potential for misusing that control.

3.2.8 Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.

3.2.9 System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

3.2.10 System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.

4 VULNERABILITY MANAGEMENT

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

4.1 GOALS AND OBJECTIVES

4.1.1 Preparation for vulnerability analysis and resolution activities is conducted.

4.1.2 A process for identifying and analyzing vulnerabilities is established and maintained.

4.1.3 Exposure to identified vulnerabilities is managed.

4.1.4 The root causes of vulnerabilities are addressed.

4.2 VULNERABILITY MANAGEMENT POLICY STATEMENTS

4.2.1 Departments shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.

5 CYBERSECURITY INCIDENT MANAGEMENT

Information Security Incident Management establishes the policy to be used by each department in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that:

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

This domain defines management controls for addressing cyber incidents. The controls provide a consistent and effective approach to Cyber Incident Response aligned with Orange County's Cyber Incident Response Plan, to include:

- Collection of evidence related to the cyber incident as appropriate
- Reporting procedures including any and all statutory reporting requirements
- Incident remediation
- Minimum logging procedures
- Annual testing of the plan

5.1 GOALS AND OBJECTIVES

5.1.1 A process for identifying, analyzing, responding to, and learning from incidents is established.

5.1.2 A process for detecting, reporting, triaging, and analyzing events is established.

5.1.3 Incidents are declared and analyzed.

5.1.4 A process for responding to and recovering from incidents is established.

5.1.5 Post-incident lessons learned are translated into improvement strategies.

5.2 CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

5.2.1 Cybersecurity incident management procedures shall be established within each department to ensure quick, orderly, and effective responses to security incidents. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan. The steps involved in managing a security incident are typically categorized into six stages:

5.2.2 System preparation

5.2.3 Problem identification

5.2.4 Problem containment

5.2.5 Problem eradication

5.2.6 Incident recovery

5.2.7 Lessons learned

5.2.8 The DISO shall act as the liaison between applicable parties during a cybersecurity incident. The DISO shall be the department's primary point of contact for all IT security issues.

5.2.9 A directory or phone tree shall be created listing all department cybersecurity incident liaison contact information.

5.2.10 Departments shall conduct periodic (at least annually) cybersecurity incident scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.

5.2.11 Departments shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, vendors and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan.

5.2.12 Each department shall familiarize its employees on the use of its cybersecurity incident reporting procedures.

5.2.13 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.

5.2.14 Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.

5.2.15 Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.

5.2.16 Departments shall report cybersecurity incidents to the Central IT Service Desk in accordance with the County's Cyber Incident Reporting Policy.

5.2.17 Confirmed cybersecurity incidents that meet the criteria defined in the Significant Incident/Claim Reporting Protocol shall be reported by the County's Chief Information Security Officer to the Chief Information Officer (CIO), County Executive Officer (CEO), and the Board of Supervisors within 24 hours of determination that a cybersecurity incident has occurred.

6 SERVICE CONTINUITY MANAGEMENT

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission. Services that are most important to an organization's ability to meet its mission are considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services.

This domain defines requirements to document, implement and annually test plans, including the testing of all appropriate cybersecurity provisions, to minimize impact to systems or processes from the effects of major failures of information systems or disasters via adoption and annual testing of:

- Business Continuity Plan
- Disaster Recovery Plan
- Cyber Incident Response Plan

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

6.1 GOALS AND OBJECTIVES

6.1.1 Service continuity plans for high-value services are developed.

6.1.2 Service continuity plans are reviewed to resolve conflicts between plans.

6.1.3 Service continuity plans are tested to ensure they meet their stated objectives.

6.1.4 Service continuity plans are executed and reviewed.

6.2 SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

6.2.1 Backups of all essential electronically-maintained County business data shall be routinely created and properly stored to ensure prompt restoration.

6.2.2 Each department shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the department.

6.2.3 The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.

6.2.4 Departments shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.

6.2.5 Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.

6.2.6 Departments shall define and periodically test a formal procedure designed to verify the success of the backup process.

6.2.7 Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.

6.2.8 Departments shall retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.

6.2.9 Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.

6.2.10 Each department shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.

6.2.11 Departments shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). As detailed in Section 14: Risk Assessment and Treatment, RAs include department identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the department has deemed critical after performing a risk analysis.

6.2.12 Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.

6.2.13 Each department shall maintain a comprehensive plan document containing its business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans shall be prepared in accordance with the standards established by the County's Business Continuity Management Policy.

6.2.14 Each department shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.