

HARBOUR WATERWAY
SPECIAL DISTRICT
Agenda

Tuesday
July 11, 2023
6:00 pm

Watson Realty
2490 Monument Road
Jacksonville, FL. 32225

- I. Introduction**
 - a. Call to Order
 - b. Roll Call / Quorum

- II. FY 2023-24 non-Ad Valorem Tax Assessment Public Hearing**

- III. Administrative**
 - a. Approval of Minutes
 - i. Minutes from May 23, 2023*

- IV. District Business**
 - a. Reed Island Spoil Site
 - i. Reed Island Nature Park – Transfer Park Property (77.7 acres) to HWSD*
 - ii. Ordinance 2023-351, Passed*
 - b. Spoil Site Disposal Activity
 - i. Isle of Palms – Dredging Project*
 - ii. Fincantieri Ship Yard – Dredging Project*
 - c. Marina – Next Steps:
 - i. Replace bulkhead and replace fixed dock next to boat ramp*
 - ii. Replace electrical service panel & upgrade security / gate*
 - iii. Extend boat ramp*
 - d. Southern Bulkhead Replacement – live wall (Marl & Limestone) or bulkhead 1,500 linear feet
 - e. Powerline Dredging Project – up to 30,000 cubic yards
 - f. Waterway Rules & Regulations
 - i. Dock Approvals*

- V. Financial**
 - a. Resolution 2023-07, approving the FY 2023-24 non-Ad Valorem assessment
 - b. Approval to disburse funds

- VI. District Schedule**
 - i. Next Scheduled Board Meeting – August 8, 2023*

- VII. Other Business**
 - a. Legal and Compliance Issues

- VIII. Comments and Questions from Audience**

- IX. Adjournment of HWSD Meeting**

HARBOUR WATERWAY SPECIAL DISTRICT

Meeting Minutes

Tuesday, July 11, 2023

I. Introduction

The Harbour Waterway Special District (HSWD) meeting of the Board of supervisors was held on July 11, 2023. The meeting was called to order at 6:00 pm. In attendance were Rick Fornos, Bob Birtalan, Wally Lovely, Mark Todd, Mike Brande and District Manager Stanley Pipes. It was noted that there was a quorum present. Harbour Waterway attorney Wayne Flowers was present. Caroline Birtalan was present as recording secretary.

II. FY 2023-24 Non- Ad Valorem Tax Assessment Public Hearing

The FY 2023-24 Public Hearing on the proposed non-Ad Valorem assessment was opened to the public for any questions, comments, or concerns. No concerns or questions were voiced by the public. The public hearing was closed.

III. Administrative

Approval of minutes from May 23, 2023 – A Motion was made to approve the meeting minutes; Motion Carried.

IV. District Business

Reed Island Nature Park- Ordinance 2023-351 was passed.

Isle of Palms- Progress is being made and the project is almost completed.

Fincantieri Shipyard- No current update.

HWSD Marina- Hayward Construction had an onsite visit to the marina to review the proposed bulkhead replacement and the extension of the boat ramp. Hayward Construction is preparing an estimate for the renovations. Remaining updates and repairs include replacing the electrical panel, upgrading security and the gate, replacing the bulkhead and capping the bulkhead with a fixed dock, and extending the boat ramp.

Southern Bulkhead- From the powerlines to the first house, the existing bulkhead needs to be repaired to prevent material from flowing from Mill Cove into the canal system. Several alternatives are being reviewed.

Powerline Dredging Project- An estimated 30,000 cubic yards need to be dredged underneath the powerlines to Canal Markers 19 / 20.

Waterway rules and regulations- No news to report.

Financial

Non-Ad Valorem Assessment- Resolution 2023-07 (FY 2023-24 non-Ad Valorem Assessment) was reviewed and discussed by the Board. A motion was made to approve Resolution 2023-07: Motion Carried.

Resolution 2023-08, Information Security Policy- A security policy was discussed by the Board, and this will protect all saved confidential information. A motion was made to approve Resolution 2023-08; Motion Carried.

Approval to disburse funds- A motion was made to approve the disbursements for administrative services, legal services, district manager billing, payroll and withholding tax, Landscape Services, Ramps for Marina, and Truist payment and fees totaling \$17,323.50; Motion Carried.

Total available funds in the HWSD general fund after disbursements is \$2,948,437.34 as of June 30,2023. Total Projected Available funds after FY Operating and Project expenses is \$1,096.277.41.


V. District Business

Next scheduled Board Meeting- The next meeting is scheduled for August 8, 2023.

Adjournment

The meeting was adjourned at 7:02 PM. The next monthly Board of Supervisors meeting is Scheduled for August 8, 2023.

Respectfully Submitted,



Caroline B. Birtalan
Recording Secretary



Robert P. Birtalan
Secretary / Treasurer

1 Introduced by the Council President at the request of the Mayor and
2 amended by the Neighborhoods, Community Services, Public Health and
3 Safety Committee:

4
5
6 **ORDINANCE 2023-351-E**

7 AN ORDINANCE APPROVING AND AUTHORIZING THE
8 MAYOR, OR HIS DESIGNEE, AND CORPORATION
9 SECRETARY TO EXECUTE AND DELIVER, FOR AND ON
10 BEHALF OF THE CITY, THAT CERTAIN AGREEMENT FOR
11 SALE AND PURCHASE ("PSA") BETWEEN THE CITY OF
12 JACKSONVILLE ("CITY") AND THE HARBOUR WATERWAY
13 SPECIAL DISTRICT ("HARBOUR"), AND TO EXECUTE ALL
14 DEEDS AND CLOSING DOCUMENTS RELATING THERETO,
15 AND AUTHORIZING ANY TECHNICAL CHANGES TO THE PSA
16 DOCUMENTS RELATING THERETO, AND OTHERWISE TAKE
17 ALL NECESSARY ACTION TO EFFECTUATE THE PURPOSE
18 OF THE PSA, FOR THE CONVEYANCE TO HARBOUR OF
19 PROPERTY LOCATED IN COUNCIL DISTRICT 2 AND AT
20 LARGE GROUP 2, COMPRISED OF APPROXIMATELY 77.7
21 ACRES OF REAL PROPERTY LOCATED ON AN
22 ISLAND/PENINSULA USED FOR DREDGE SPOIL AND KNOWN
23 AS REED ISLAND IN THE ST. JOHNS RIVER SOUTH OF
24 BLOUNT ISLAND LESS THAN FOUR MILES WEST OF THE
25 INTRACOASTAL WATERWAY (THE "PROPERTY") IN
26 EXCHANGE FOR HARBOUR'S AGREEMENT TO MANAGE AND
27 IMPROVE AND EXPAND THE PUBLIC PARK LOCATED ON
28 THE PROPERTY; PROVIDING FOR WAIVER OF SECTION
29 122.422 (DETERMINATION OF NEED; DECLARATION THAT
30 PROPERTY IS SURPLUS TO THE NEEDS OF THE PUBLIC),
31 *ORDINANCE CODE*, AS TO DECLARING THE PROPERTY

1 SURPLUS; PROVIDING FOR WAIVER OF SECTION
2 122.421(B) (GENERAL PROVISIONS; DELEGATION OF
3 AUTHORITY), *ORDINANCE CODE*, AS TO REPLACING
4 PROPERTY WITH SIMILAR PARK LAND; APPROPRIATING
5 \$375,000.00 FROM THE REED ISLAND CONSTRUCTION
6 PHASE FLORIDA INLAND NAVIGATION DISTRICT (FIND)
7 GRANT PROJECT TO FUND A SHORTFALL IN THE REED
8 ISLAND DESIGN PHASE FIND GRANT PROJECT
9 (\$39,681.59) AND TO FUND THE JOE CARLUCCI BOAT
10 RAMP FISHING PIER PROJECT (\$335,318.41);
11 AMENDING THE 2023-2027 FIVE-YEAR CAPITAL
12 IMPROVEMENT PLAN APPROVED BY ORDINANCE
13 2022-505-E TO REDUCE FUNDING FOR THE REED ISLAND
14 FIND GRANT PROJECTS AND TO INCREASE FUNDING FOR
15 THE JOE CARLUCCI BOAT RAMP FISHING PIER PROJECT;
16 PROVIDING FOR CITY OVERSIGHT BY THE PARKS,
17 RECREATION AND COMMUNITY SERVICES DEPARTMENT;
18 AMENDING ORDINANCE 2010-725-E, AS AMENDED BY
19 ORDINANCES 2015-233-E and 2020-267-E; PROVIDING
20 AN EFFECTIVE DATE.

21
22 **BE IT ORDAINED** by the Council of the City of Jacksonville:

23 **Section 1. Agreement for Sale and Purchase Approved and**
24 **Execution Authorized.** There is hereby approved, and the Mayor, or
25 his designee, and Corporation Secretary are hereby authorized to
26 execute and deliver, for and on behalf of the City, the PSA between
27 the City and Harbour, in substantially the same form as attached
28 hereto as **Revised Exhibit 1**, labeled as "Revised Exhibit 1, Rev
29 Agmt, June 20, 2023 - NCSPHS" (with such "technical" changes as herein
30 authorized), and to execute all deeds and closing documents relating
31 thereto, and otherwise take all action necessary or appropriate to

1 effectuate the purpose of this Ordinance.

2 The PSA is for the purchase by Harbour of approximately 77.7
3 acres of real property owned by the City and the consideration for
4 transfer of the Property to Harbour, Harbour will manage, maintain
5 and improve the Property as provided in the PSA. The Property to be
6 conveyed is shown on the map attached as **Exhibit 2** and will be used
7 by Harbour as a public access park facility except as consistent with
8 the terms of the PSA.

9 The PSA may include such additions, deletions, and changes as
10 may be reasonable, necessary, and incidental for carrying out the
11 purposes thereof, as may be acceptable to the Mayor or his designee,
12 with such inclusion and acceptance being evidenced by execution of
13 the PSA by the Mayor or his designee. No modification of the PSA may
14 increase the financial obligations or the liability of the City and
15 any such modification shall be technical only and shall be subject
16 to appropriate legal review and approval of the General Counsel or
17 his or her designee and all other appropriate action required by law.
18 For the purposes of this Ordinance, "technical changes" is defined
19 as those changes having no financial impact to the City; including,
20 but not limited to, changes in legal descriptions or surveys,
21 resolution of title defects (if any), descriptions of infrastructure
22 improvements and/or any road project, ingress and egress, easements
23 and rights-of-way, performance schedules (provided that no
24 performance schedule may be extended for more than one year without
25 City Council approval), design standards, access and site plans, and
26 other non-substantive changes that do not substantively increase the
27 duties and responsibilities of the City under the provisions of the
28 PSA.

29 **Section 2. Waiver of Section 122.422 (Determination of**
30 **need; declaration that property is surplus to the needs of the**
31 **public), Ordinance Code.** Section 122.422 (Determination of need;

1 declaration that property is surplus to the needs of the public),
2 Chapter 122 (Public Property), *Ordinance Code*, is hereby waived as
3 to the process of declaring the property surplus to the needs of the
4 City by circulating the property to each City agency to determine
5 whether there is a need.

6 **Section 3. Waiver of Section 122.421(b) (General**
7 **provisions; delegation of authority), *Ordinance Code*.** Section
8 122.421(b) (General provisions; delegation of authority), Chapter 122
9 (Public Property), *Ordinance Code*, is hereby waived as to allow for
10 sale of the City park to Harbour without the City replacing the park
11 land with new park land of equal or greater size and value.

12 **Section 4. Appropriation.** For the 2022-2023 fiscal year,
13 within the City's budget, there is hereby appropriated the indicated
14 sum from the account listed in subsection (a) to the account listed
15 in subsection (b):

16 (The account information is attached hereto as **Exhibit 3** and
17 incorporated herein by this reference)

18 (a) Appropriated from:

19 See **Exhibit 3** \$375,000.00

20 (b) Appropriated from:

21 See **Exhibit 3** \$375,000.00

22 (c) Explanation of Appropriation:

23 The funding above represents: a) a deappropriation of
24 \$750,000.00 from the Florida Inland Navigation District
25 (FIND) Reed Island construction phase project, consisting
26 of a City match of \$375,000.00 and FIND grant funding of
27 \$375,000.00, b) a deappropriation of \$100,000.00 in the
28 FIND Reed Island design phase project construction account
29 and an appropriation of \$39,681.59 to the FIND Reed Island
30 design phase project City match account (for a net
31 deappropriation of \$60,318.41 within the design phase

1 project), and c) an appropriation of \$335,318.41 to the
2 Joe Carlucci Boat Ramp Fishing Pier project all as further
3 detailed in Section 5 below.

4 **Section 5. Purpose.** The purpose of the appropriation in
5 Section 4 is to reallocate unused City matching dollars that were
6 previously budgeted for the FIND Reed Island construction phase
7 project to: a) cover the shortfall in the FIND Reed Island design
8 phase project, and b) appropriate funding for the Joe Carlucci Boat
9 Ramp Fishing Pier project. The City previously approved and
10 appropriated funding for both the design and construction phases of
11 the FIND Reed Island project. As a result of the conveyance of the
12 Property to Harbour, the City will not be eligible to seek
13 reimbursement from FIND for expenditures already incurred for the
14 design phase of that project and the City will not be commencing the
15 construction phase of the project for which no expenditures have been
16 incurred. The City has incurred expenditures for the design phase of
17 the project in excess of the City matching dollars appropriated for
18 that phase, leaving a funding shortfall of \$39,681.59 in the design
19 phase project. However, as a result of not commencing the construction
20 phase of the project, there exists unused City matching funds of
21 \$450,000.00. This legislation reallocates a portion of the unused
22 City matching funds of the construction phase project (\$375,000.00)
23 to: a) increase the City match for the design phase project
24 (\$39,681.59) in order to cover the funding shortfall within that
25 phase and b) appropriate \$335,318.41 for the Joe Carlucci Boat Ramp
26 Fishing Pier project. Additionally, as part of the appropriation in
27 Section 4, the expenditure budget for the design phase project is
28 being reduced by \$60,318.41 to close out the project and the
29 expenditure budget for the construction phase project is being reduced
30 by \$750,000.00. The remaining balance of \$75,000.00 within the
31 construction phase project has been identified for a future planned

1 appropriation.

2 **Section 6. Capital Improvement Plan Amendment.** Ordinance
3 2022-505-E, adopting the 2023-2027 Five-Year Capital Improvement Plan
4 (the "CIP") for the City and certain of its independent agencies, is
5 hereby amended to reduce funding for the projects entitled FIND -
6 Reed Island Dock & Dev Design (design phase) and FIND Reed Island -
7 PRC14619 (construction phase), and increase funding for the Joe
8 Carlucci Boat Ramp Fishing Pier project as more fully described in
9 the Project Information Sheets attached hereto as **Exhibit 4** and
10 incorporated herein by this reference. The City Council finds that
11 the deferral of this amendment of the CIP until the next annual budget
12 and CIP review will unnecessarily delay the improvements at the Joe
13 Carlucci Boat Ramp at Sisters Creek which will enhance public fishing
14 access at this waterfront park and alleviate conflicts between boaters
15 and fishermen.

16 Pursuant to Section 122.605(c), *Ordinance Code*, enactment of
17 this Ordinance requires the affirmative vote of two-thirds of the
18 City Council members present at the meeting because of the CIP
19 amendment set forth in this section. This Ordinance shall constitute
20 an amendment to Ordinance 2022-505-E. In all other respects, the
21 Five-Year Capital Improvement Plan approved by Ordinance 2022-505-E
22 shall remain unchanged and continue in full force and effect.

23 **Section 7. Oversight.** The Parks, Recreation and Community
24 Services Department shall provide oversight and administration of the
25 PSA.

26 **Section 8. Amendment to Section 2, Ordinance No.**
27 **2010-725-E, as amended by Ordinance Nos. 2015-233-E and 2020-267-E.**
28 Section 2 is amended in part to read as follows:

29 Sec. 2. Purpose. The purpose of the District shall be the
30 continuing maintenance of the system of canals located in The Harbour
31 neighborhood, Harbour Cay neighborhood, Harbour North neighborhood,

1 Harbour Island neighborhood, construction and maintenance of a dredge
2 disposal site, ~~and~~ maintenance and improvement of the upland and
3 marsh areas surrounding the spoil disposal site together with access
4 roads to the spoil disposal site, and maintenance and operation of
5 public park property adjacent to the spoil disposal site conveyed to
6 the District by the City for operation as a park. The District shall
7 fulfill its purpose by dredging the canals, dredging the channel that
8 provides the canals with access to the St. Johns River, maintaining
9 a jetty, maintaining navigational aids, enhancing and restoring
10 uplands and wetlands on the lands owned by the District, and operating
11 and maintaining a public access park on land adjacent conveyed to the
12 District for that purpose that are adjacent to the spoil site owned
13 and operated by the District.

14 **Section 9. Retroactive applicability.** This Ordinance shall
15 be retroactive so that the amendment adopted herein shall be effective
16 as if it were contained in the original enabling Ordinance 2010-725-E.

17 **Section 10. All other aspects of Ordinance 2010-725-E**
18 **unchanged.** With the exception of Section 9 of this Ordinance, in all
19 other respects Ordinance 2010-725-E shall remain unchanged and in
20 full force and effect.

21 **Section 11. Further Action Authorized.** The General Counsel,
22 or his designee, is authorized to take such further action and to
23 execute all other documents necessary to effect the intentions set
24 forth herein.

25 **Section 12. Effective Date.** This Ordinance shall become
26 effective upon signature by the Mayor or upon becoming effective
27 without the Mayor's signature.

1 Form Approved:
2

3 /s/ Mary E. Staffopoulos

4 Office of General Counsel

5 Legislation Prepared By: Harry M. Wilson, IV

6 GC-#1573926-v1-2023-351-E.docx

AGREEMENT FOR SALE AND PURCHASE

THIS AGREEMENT is between CITY OF JACKSONVILLE, a political subdivision and municipal corporation existing under the laws of the state of Florida, whose address is 117 W. Duval Street, Suite 400, Jacksonville, Florida 32202, as "Seller," and the HARBOUR WATERWAY SPECIAL DISTRICT, a dependent Special District created by the City of Jacksonville, Florida, through Ordinance No. 2010-725-E, whose mailing address is 11554 Starboard Drive, Jacksonville, Florida, 32225, as "Buyer".

1. PURCHASE AND SALE. For good and valuable consideration, the receipt of which is hereby acknowledged, Seller hereby agrees to sell to Buyer and Buyer agrees to purchase from Seller the real property located in Duval County, Florida, identified as Real Estate Parcel Nos. 160258- 0010 & 160258-0004, and more particularly described in Exhibit "A" attached hereto, together with all timber, transferable development rights, improvements, easements, appurtenances, hereditaments, and riparian and littoral rights, if any (the "Property"), and subject to the covenants referenced in Section 3.B below, which shall be covenants and restrictions set forth in the deed from Seller to Buyer described in paragraph 8 below. This Agreement becomes legally binding upon the approval of each party's governing board and due execution of same, the later date of which will be the "Effective Date" of this Agreement.

2. USE OF THE PARK PROPERTY. The segment of the Property described in Exhibit "B") will be solely used as a park / conservation area by Buyer (hereinafter "Park Property), who will allow the general public to utilize the existing and proposed park amenities, including docks, picnic pavilions, nature trails, and roadways in perpetuity. The Park Property and all facilities within shall be open daily to the general public during daylight hours, provided, however, that access to the Park Property shall be limited to water access only.

3.A. PURCHASE PRICE. The purchase price for the Property shall be One Dollar (\$1.00) together with Buyer's agreement at its sole cost (i) to construct the park facilities identified as "Consideration for Conveyance" in Section 3.B below and (ii) to maintain the Park Property in perpetuity. No additional consideration shall be paid by Buyer for conveyance of the Property.

3.B. CONSIDERATION FOR CONVEYANCE. All of the items set forth in this paragraph 3.B comprise the consideration for the conveyance of the Property from Seller to Buyer. Buyer shall perform the items set forth in subparagraphs 3.B(i) through 3.B(viii), and item 3.B(x), at its sole cost and expense:

(i) Buyer agrees to increase the size of the Park Property from 77.7 acres to a total of at least 82.2 acres by adding properties currently owned by Buyer which will include wetlands and tidal salt marsh contiguous to the Park Property as shown in Exhibit "B".

(ii) Buyer agrees to excavate a 100 foot wide canal to a depth of -5.0 feet MLW within 300 feet of the picnic pavilions as shown on the site plan attached as Exhibit "C". Buyer agrees to construct a bulkhead on both sides of the canal and maintain the bulkhead indefinitely. The canal shall be periodically dredged, as appropriate to maintain a navigable depth in order for appropriately sized boats to dock at the Park Property. Buyer intends for the canal to eventually be connected to a private canal system adjacent to the Property allowing egress by water for residential parcels on the private waterway, subject to permitting and approval from the USACE and the FDEP, but Buyer's intended development of this private canal system is not consideration for Seller's conveyance of the Property.

(iii) Buyer agrees to construct and maintain an ADA complaint 8' x 125' floating dock with an ADA complaint gangway and walkways to allow egress from the floating dock to the picnic pavilions as shown in Exhibit "C". Docks and bulkheads shall be inspected monthly to identify maintenance needs and repairs. Buyer shall use commercially reasonable efforts to repair any defects or repairs identified during

inspections within (1) one year, and minor repairs shall be corrected as quickly as possible.

(iv) Buyer agrees to construct and maintain two (2) picnic pavilions per the attached specifications as shown in Exhibit "D," and to grade and maintain a beach area along the St Johns River adjacent to the picnic pavilions.

(v) Buyer agrees to maintain at least 4000 linear feet of nature trails, not to exceed eight (8) feet in width on the Park Property. Nature trail maintenance shall include mowing the trails up to 2 times per month from April thru October and once per month November thru March or as needed; occasionally trimming along the trails to remove impediments; and installing and maintaining trail signage. Park signage shall include the park rules sign, park trail map, trail directional signage, and any advisable warning signs posted at the picnic pavilions.

(vi) Buyer agrees to install a three-strand barbed wire fence adjacent to the dredge material management area to deter park visitors from accessing the dredge spoil site.

(vii) Any buildings to be constructed on Park Property shall be limited to those facilities included in the conceptual plan attached hereto as Exhibit "C." Any other buildings proposed for construction in the Park shall require prior written approval from the City of Jacksonville's Director of Parks, Recreation and Community Services (the "Parks Director").

(viii) Buyer agrees to continue removal of invasive and nuisance plants, it is understood that Buyer or its agents will clear and burn or allow the debris to decay naturally, on-site. Buyer will follow best management practices in conducting this activity and where appropriate and necessary will utilize herbicide(s) to fully eradicate target plants. Buyer agrees to continue to collaborate with the City of Jacksonville, U.S. Army Corp of Engineers, and the First Coast Invasive Working Group to work towards eradication of Tamarix and Brazilian Pepper from the Buyer's existing property and the Park Property.

(ix) The name of the Park Property shall be "Reed Island Park" and any subsequent Park name change requires the written approval of the Parks Director.

(x) Buyer will seek to obtain necessary property interest to provide access to the Park Property by a service road south of the Buyer's property as shown on the Map attached as Exhibit "B". If and to the extent Buyer does secure legal access to the Park Property via a roadway, it will permit and authorize Seller, its agents and employees to utilize such access for purposes of inspecting the Park Property. However, said access, if obtained, shall not be utilized for public access to the Park Property.

(xi) The Buyer shall not sell or convey any of the 82.2-acre Park Property without prior written consent of the Parks Director, which consent shall not be unreasonably withheld.

(xii) The foregoing subsections 3.B.(i)-(xi), shall survive the closing of the sale of the Property to Buyer, shall supersede subsections 3.B(ii)-(vi) of that certain Sale and Purchase Agreement executed by the parties on April 23, 2019 and shall be set forth as covenants in the deed from Seller to Buyer described in paragraph 8.

4. **INSPECTION PERIOD/ENVIRONMENTAL SITE ASSESSMENT.** Buyer shall have the right, at its sole cost and expense, to inspect the Property and to conduct an environmental site assessment of the Property to determine the existence and extent, if any, of any Hazardous Materials on the Property during the thirty (30) day period immediately following the Effective Date of this Agreement (the "Inspection Period"). Prior to expiration of the Inspection Period, Buyer may cancel this Agreement for any reason without penalty, except that Buyer shall restore any property disturbed by its inspections and assessments to the condition the property was in prior to Buyer's inspections and assessments. If further investigations, testing, monitoring or environmental site assessments are required by Buyer to determine the existence or extent of Hazardous Materials on the Property, Buyer may conduct such procedures at the Buyer's sole cost and expense. For purposes of this Agreement "Hazardous Materials"

shall mean any hazardous or toxic substance, material or waste of any kind or any other substance which is regulated by any Environmental Law (as hereinafter defined in paragraph 5.)

5. HAZARDOUS MATERIALS. If the environmental site assessment provided for in paragraph 4 confirms the presence of Hazardous Materials on the Property, Buyer, at its sole option, may elect to terminate this Agreement and neither party shall have any further obligations under this Agreement. Should Buyer elect not to terminate this Agreement or fails to obtain an environmental site assessment of the Property, then Buyer shall accept the Property "as is, where is, and with all faults", together with all defects, latent and patent, if any. Seller shall have no duty to pursue and or accomplish any clean-up of the Hazardous Materials or to otherwise bring the Property into compliance with Environmental Law. "Environmental Law" shall mean all federal, state and local laws, including statutes, regulations, ordinances, codes, rules, judgments, orders, decrees, permits, concessions, grants, franchises, licenses, agreements and other governmental restrictions relating to the protection of the environment or human health, welfare or safety, or to the emission, discharge, seepage, release or threatened release of any contaminant, solid waste, hazardous waste, pollutant, irritant, petroleum product, waste product, radioactive material, flammable or corrosive substance, carcinogen, explosive, polychlorinated biphenyl, asbestos, hazardous or toxic substance, material or waste of any kind into the environment, including, without limitation, ambient air, surface water, ground water, or land including, but not limited to, the Federal Solid Waste Disposal Act, the Federal Clean Air Act, the Federal Clean Water Act, the Federal Resource and Conservation and Recovery Act of 1976, the Hazardous and Solid Waste Amendments of 1984, the Federal Comprehensive Environmental Response, Compensation and Liability Act of 1980, the Federal Superfund Amendments and Reauthorization Act of 1986, Chapters 161, 253, 373, 376 and 403, Florida Statutes, Rules of the U.S. Environmental Protection Agency, Rules of the Florida Department of Environmental Protection, and the rules of the Florida water management districts now or at any time hereafter in effect.

No later than thirty (30) days following the Effective Date, Seller will provide Buyer with any information, reports, or data requested by Buyer and after reasonable inquiry by Seller found to be in Seller's possession regarding soil or water quality on the Property or the presence of hazardous materials, as defined above, on the Property.

If Buyer elects not to terminate this Agreement or fails to obtain an environmental site assessment of the Property, and proceeds to Closing as provided above, Buyer shall indemnify to the extent permitted by law, Seller, its officers, servants, agents and employees from and against any and all claims, suits, actions, damages, liabilities, expenditures or causes of action of whatsoever kind arising from Hazardous Materials placed on the Property prior to closing. Buyer shall defend, at Buyer's sole cost and expense, any legal action, claim, or proceeding instituted by any person against Seller as a result of any claim, suit, or cause of action for injuries to body, life, limb, or property for which Hazardous Materials placed on the Property prior to closing are alleged to be a contributing legal cause.

6. Intentionally Deleted.

7. DEFECTS IN TITLE. If the title insurance commitment or Survey obtained pursuant to this Agreement disclose any defects in title arising from liens against the Property, such liens up to the amount of Seller's net proceeds from the sale shall be satisfied at closing by Seller. If the title insurance commitment or Survey disclose any other defects that are not acceptable to Buyer, Buyer shall have the option to either: (a) accept the title as it then is with no reduction in the Purchase Price, or (b) terminate this Agreement, thereupon releasing Buyer and Seller from all further obligations under this Agreement. Seller shall have no duty to cure any title defects arising from other than liens against the Property.

8. INTEREST CONVEYED; NO WARRANTIES. At closing, Seller shall execute and deliver to Buyer a quitclaim deed conveying Seller's interest in the Property "as is, where is, and with all faults", and subject to (i) a restriction that the Property be used for residential non-commercial dredge spoil disposal and reclamation or for conservation, and for no other purposes, (ii) the covenants in paragraph 3B of this Agreement, and (iii) the right of re-entry described in paragraph 14. Seller has made no representations

or warranties of any nature whatsoever, express or implied, regarding the Property, including but not limited to the physical and environmental condition of the Property, the zoning of the Property, title to the Property, the suitability of the Property or any improvements for Buyer's intended purpose; or Buyer's legal ability to use the Property for Buyer's intended use.

9. PREPARATION OF CLOSING DOCUMENTS. Buyer shall prepare the deed described in paragraph 8 of this Agreement and Buyer's and Seller's closing statements. Buyer understands Seller, as an agency of the state, is unable to execute a no-lien affidavit customarily required to delete the standard exceptions from the title insurance policy. Seller will cooperate with the agent for the title insurance company to provide such reasonable, alternative evidence within the Seller's legal capacity to provide and at no expense to Seller to enable the title agent to delete the standard exceptions typically deleted by a no-lien affidavit.

10. EXPENSES. Buyer will pay the documentary stamp tax, if any, and all other taxes or costs associated with the conveyance, including the cost of recording the deed described in paragraph 8 of this Agreement.

11. TAXES AND ASSESSMENTS. Seller and Buyer are exempt from taxation. At closing, Seller shall satisfy any assessments for which it is legally responsible, if any, prorated to the date of Closing, that are or may become a lien against the Property.

12. CLOSING PLACE AND DATE. The closing shall be on or before forty-five (45) days after the Effective Date, unless earlier terminated pursuant the provisions of paragraphs 4 above. The parties shall mutually set the date, time and place of closing.

13. RISK OF LOSS AND CONDITION OF PROPERTY. Seller assumes all risk of loss or damage to the Property prior to the date of closing. The Property shall be transferred and conveyed to Buyer in the same or essentially the same condition as of the date of Seller's execution of this Agreement, ordinary wear and tear excepted. If the condition of the Property is altered, by an act of God or other natural force beyond the control of Seller, however, Buyer may elect, at its sole option, to terminate this Agreement and neither party shall have any further obligations under this Agreement.

14. RIGHT OF RE-ENTRY CLAUSE. In the event the Buyer fails to execute the terms and conditions set forth in Section 3B (ii thru vi) within three (3) years of the closing date, Seller may, at its option, exercise a right of re-entry as to the Park Property" including any improvements then located thereon, such that 1) Seller shall convey the Park Property to the City of Jacksonville, and 2) all proceeds obtained from the sale of residential parcels 1 thru 4 located on the St. John River and depicted in Exhibit "B" shall be paid to the City of Jacksonville; or, if such remedy is unavailable, Buyer shall convey title to any such parcels it holds to City of Jacksonville within ten (10) business days' written notice. In addition, if Buyer fails to maintain the Park Property as specified in Section 3B, including maintaining the facilities listed herein, and has not cured any material deficiencies within one (1) year of written notice from the City of Jacksonville, Buyer shall convey the Park Property to the City of Jacksonville at Seller's sole election. The rights of re-entry set forth herein shall be set forth in the Deed from Seller to Buyer described in Paragraph 8 above.

15. ACCESS. Seller makes no warranties as to whether there is legal and practical ingress and egress for the Property over public roads or valid, recorded easements for the use and benefit of and as an appurtenance to the Property.

16. BROKERS. No persons, firms, corporations or other entities are entitled to a real estate commission or other fees as a result of this Agreement or subsequent closing. Buyer shall indemnify and hold Seller harmless from any and all such claims.

17. RECORDING. This Agreement may not be recorded.

18. ASSIGNMENT. This Agreement may not be assigned.

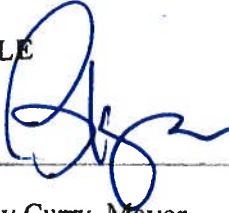
19. TIME. Time is of essence with regard to all dates or times set forth in this Agreement.
20. SEVERABILITY. If any of the provisions of this Agreement are deemed to be unenforceable and the unenforceability of said provisions does not adversely affect the purpose and intent of this Agreement, the enforceability of the remaining provisions of this Agreement shall not be affected.
21. SUCCESSORS IN INTEREST. This Agreement shall bind and inure to the benefit of Seller and Buyer and their respective legal representatives and successors. Whenever used, the singular shall include the plural and one gender shall include all genders.
22. ENTIRE AGREEMENT. This Agreement contains the entire agreement between the parties pertaining to the subject matter contained in it and supersedes all prior and contemporaneous agreements, representations and understandings of the parties. No supplement, modification or amendment to this Agreement shall be binding unless executed in writing by the parties.
23. WAIVER. Failure of either party to insist upon strict performance of any covenant or condition of this Agreement, or to exercise any right herein contained, shall not be construed as a waiver or relinquishment for the future of any such covenant, condition or right; but the same shall remain in full force and effect.
24. COUNTERPARTS. This Agreement may be executed in one or more counterparts, but all such counterparts, when duly executed, shall constitute one and the same Agreement.
25. ADDENDUM. Any addendum attached hereto that is signed by the parties shall be deemed a part of this Agreement.
26. NOTICE. Whenever either party desires or is required to give notice unto the other, it must be given by written notice, and either delivered personally, transmitted via facsimile transmission, mailed postage prepaid, or sent by overnight courier to the appropriate address indicated on the first page of this Agreement, or such other address as is designated in writing by a party to this Agreement.
27. SURVIVAL. The covenants, warranties, representations, and undertakings of the parties set forth in this Agreement shall survive the closing, the delivery and recording of the deed described in paragraph 8 of this Agreement, and Buyer's possession of the Property.
28. SOVEREIGN IMMUNITY. The Parties intend to avail themselves of the benefits of Section 768.28, Florida Statutes, and any other statutes and common law governing sovereign immunity to the fullest extent possible. Neither this provision nor any other provisions of this Agreement shall be construed as a waiver of sovereign immunity by any of the Parties.
29. NO THIRD PARTY BENEFICIARIES. Nothing in this Agreement is intended to inure to the benefit of any third party for the purpose of allowing any claim which would otherwise be barred under the doctrine of sovereign immunity.
30. FORCE MAJEURE. No failure, delay or default in performance of any obligation of a party to this Agreement shall constitute an event of default or a breach of this Agreement, or, give rise to any remedy hereunder, to the extent that such failure to perform, delay or default arises out of a cause, existing or future, that is beyond the reasonable control and without negligence of the party otherwise chargeable with failure, delay or default, including, but not limited to: action or inaction of governmental, civil or military authority; flood; fire; war; riot; earthquake; natural disaster; act, negligence or default of the other party. The affected party shall take reasonable action to minimize the consequences of any such cause. This subsection shall in no way limit the right of either party to this Agreement to make any claim against third parties for any damages suffered due to said causes.

IF THIS AGREEMENT IS NOT FULLY EXECUTED AS PROVIDED HEREIN ON OR BEFORE DECEMBER 31, 2023, NEITHER SELLER NOR BUYER SHALL BE UNDER ANY OBLIGATION TO SELL OR PURCHASE THE PROPERTY. SELLER'S PERFORMANCE AND OBLIGATION TO PAY ANY SUMS DUE UNDER THIS AGREEMENT IS CONTINGENT UPON AN ANNUAL APPROPRIATION FOR SUCH PURPOSE.


Signatures appear on the following page

SELLER

CITY OF JACKSONVILLE

By:  Brian Hughes
Chief Administrative Officer
For: Mayor Lenny Curry
Under Authority of:
Executive Order No: 2019-02

Attest:


James R. McCain, Jr.
Corporation Secretary



(OFFICIAL SEAL)

Form Approved:

By: 
Office of General Counsel

6/29/2023

Date signed by Seller

GC-#1570224-v1-Reed_island_Purchase_Agreement_05-12-2023_(ogc_revisions).docx

BUYER

HARBOUR WATERWAY SPECIAL DISTRICT

By: Wallace Lovely
Wallace Lovely
As: Chair, Board of Supervisors

Stanley H. Papp, Jr.
Witness as to Buyer

Mary Lovely
Witness as to Buyer

6/28/2023
Date signed by Buyer

EXHIBITS

- Exhibit A Property – Parcel 160258 0010 & 0004 and Legal Description
- Exhibit B Park Property and Legal Description
- Exhibit C Conceptual Site Plan – Picnic Pavilions and Floating Dock
- Exhibit D Picnic pavilions specifications

Exhibit "A"

Page 1 of 4

VOL 4231 PG 1175

31354-RG

OFFICIAL RECORDS

THIS DEED, Made this 15th day of July, A. D., 1976, between SEABOARD COAST LINE RAILROAD COMPANY, a Virginia corporation, hereinafter called "Grantor"; the CITY OF JACKSONVILLE, a municipal corporation under the laws of the State of Florida, with mailing address 220 East Bay Street, Jacksonville, Florida, 32202, hereinafter called "Grantee"; and MERCANTILE-SAFE DEPOSIT AND TRUST COMPANY, as successor Corporate Trustee under the First Mortgage dated as of January 1, 1946, made by the former Seaboard Air Line Railroad Company, to which Seaboard Coast Line Railroad Company is successor by merger;

(Wherever used herein, the terms "Grantor" and "Grantee" shall be construed in the singular or plural as the context may require or admit and shall include the heirs, legal representatives and assigns of individuals and the successors and assigns of corporations.)

WITNESSETH: Grantor, being interested in and desiring to assist in the further development of the public welfare of Grantee, has donated, granted, remised and released, and by these presents does donate, grant, remise and release unto Grantee forever those certain tracts or parcels of land situate, lying and being at Jacksonville, County of Duval, State of Florida, and described as follows, to wit:

Parcel 1: Portions of Lots 1, 2, 3 and 4 of East Greeleyville, as recorded in Deed Book "A0", Page 101, of the Public Records of said County and State, said portions of lots being in the S $\frac{1}{4}$ of Section 7, Township 2 South, Range 27 East, more particularly described as follows: Beginning at the point of intersection of the southwesterly boundary line of Grantor's right of way for its Composite-Export Terminal main track and the westerly line of Haines Street, as now established; running thence southwardly along said westerly street line 165 feet, more or less, to a corner; thence South 89° 27' 26" West 100 feet; thence North 0° 16' 40" West 194 feet, more or less, to said right of way boundary line; thence southeastwardly along said right of way boundary line 104 feet, more or less, to the point of beginning; containing 0.41 of an acre, more or less, and being indicated on print of Grantor's drawing dated June 4, 1976, attached hereto and made a part hereof; SUBJECT, However, to that certain easement dated November 15, 1972, granted by Grantor to Jacksonville Transportation Authority for service road construction.

Parcel 2: A portion of the SE $\frac{1}{4}$ of Section 30, Township 1 South, Range 28 East, of said County and State, being more particularly described as follows: The easternmost 21.97 acres of the following described tract or parcel of land: Beginning at the southeast corner of said Section 30; running thence westwardly along the south line of said Section 30, 2,332.23 feet, more or less, to the southwest corner of the "Approved Swamp Selection" according to survey by the Bureau of Land Management, U.S. Department of Interior, accepted October 5, 1949; thence northeastwardly along the northerly line of said Approved Swamp Selection 990 feet, more or less, to a corner in the northerly line of said Approved Swamp Selection; thence northeastwardly along said northerly line 2,310 feet, more or less, to the easterly line of said Section 30; thence southwardly along said east line 2,359.89 feet, more or

RETURN TO: P.S. COPE
1300 CITY HALL
JMA. F.M.

This instrument was prepared by
John T. Albritton, Jr.
Attorney
500 Water St., Jacksonville, Fla.

less, to the point of beginning; the land hereby conveyed being indicated on print of Grantor's drawing prepared by Robert M. Angas and Associates, dated May, 1962, attached hereto and made a part hereof; SUBJECT, However, to that certain perpetual easement dated April 27, 1950, granted by the Seaboard Air Line Railroad Company to the United States of America for spoil disposal purposes, recorded in Deed Book 1441, Page 568 of the Current Public Records of said County and State.

TOGETHER with all and singular the rights, members, hereditaments and appurtenances to said premises belonging or in anywise incident or appertaining.

TO HAVE AND TO HOLD said premises unto Grantee in fee simple forever; SUBJECT, However, to reservations, conditions, restrictions and easements of record.

Except as to the matters referred to in the preceding paragraph, Grantor hereby binds itself that the premises are free from encumbrances, that it is seized of said premises in fee and that it will fully warrant and forever defend all and singular said premises unto Grantee against Grantor and all other persons lawfully claiming or to claim the same or any part thereof.

Parcel 2 herein conveyed is subject to the lien of the First Mortgage made by the former Seaboard Air Line Railroad Company, dated as of January 1, 1946, as supplemented and modified, under which mortgage Mercantile-Safe Deposit and Trust Company is the present successor Corporate Trustee, and Trustee joins herein for the purpose of releasing Parcel 2 hereinabove conveyed and does hereby release Parcel 2 herein conveyed from the lien of said mortgage pursuant to the provisions of Section 6 of Article Twelve thereof; and Trustee certifies that C. E. Heinmuller retired as Individual Trustee under the aforesaid mortgage effective as of August 1, 1970, and since that date, Mercantile-Safe Deposit and Trust Company has been and is presently the Trustee acting under the aforesaid mortgage, as supplemented and modified.

The recitals of fact made herein are to be taken only as recitals made by Grantor and not by Trustee.

IN WITNESS WHEREOF Grantor and Trustee have caused these presents to be duly signed and sealed, the day and year first above written.

Signed, sealed and delivered
in the presence of:

SEABOARD COAST LINE RAILROAD COMPANY

J. W. Adams
E. J. Adams

By J. W. Adams
Vice President

Attest: H. W. Martens
H. W. Martens Assistant Secretary

Signed, sealed and delivered
in the presence of:

MERCANTILE-SAFE DEPOSIT AND TRUST
COMPANY, as successor Corporate Trustee
as aforesaid.

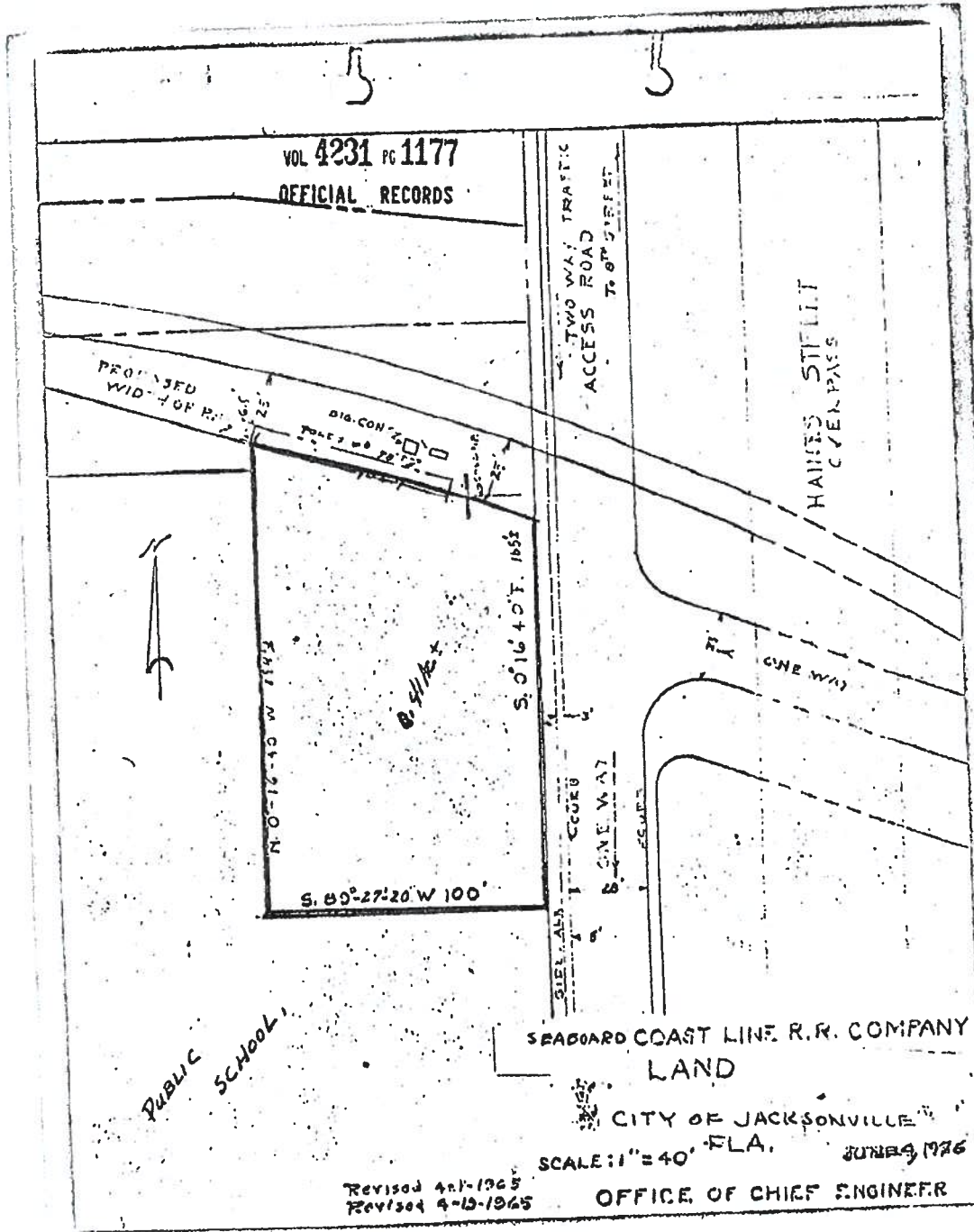
Sharon Anderson
Lawrence H. Gilbert

By A. F. Safford
Vice President

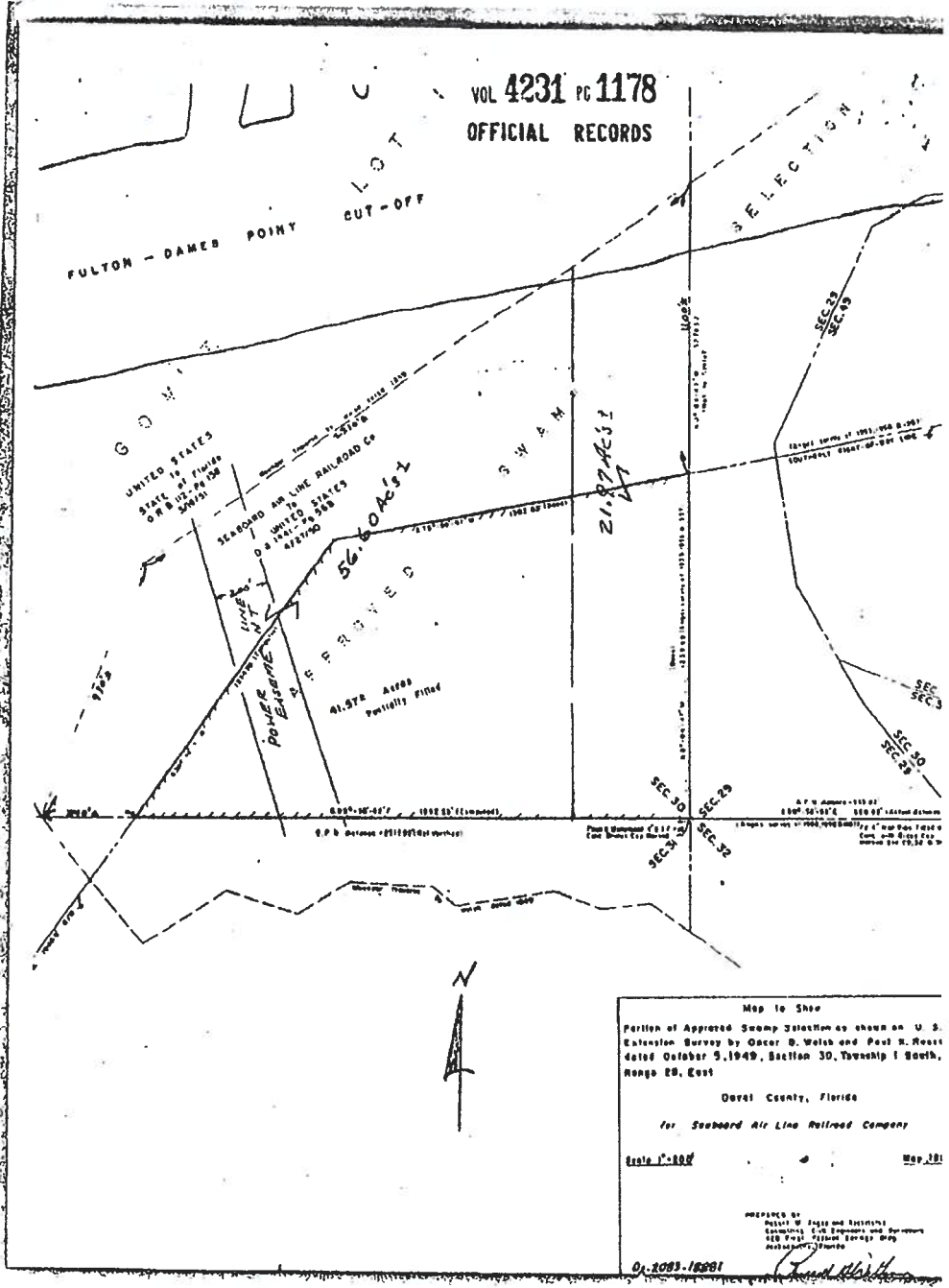
Attest: J. E. ...
Corporate Trust Officer

EXHIBIT "A"

PAGE 3 OF 4



VOL 4231 PG 1178
OFFICIAL RECORDS



MAP SHOWING A SKETCH AND DESCRIPTION OF:

PARCEL A

A PORTION OF SECTIONS 30 AND 31, TOWNSHIP 1 SOUTH, RANGE 28 EAST, DUVAL COUNTY, FLORIDA, BEING MORE PARTICULARLY DESCRIBED AS FOLLOWS.

FOR A POINT OF REFERENCE, COMMENCE AT THE SOUTHEAST CORNER OF SECTION 30, TOWNSHIP 1 SOUTH, RANGE 28 EAST, DUVAL COUNTY, FLORIDA; THENCE NORTH 89°15'09" WEST, ALONG THE SOUTH LINE OF SAID SECTION 30, A DISTANCE OF 150.00 FEET TO THE POINT OF BEGINNING;

FROM SAID POINT OF BEGINNING, THENCE SOUTH 00°01'52" EAST, 425 FEET MORE OR LESS, TO THE MEAN HIGH WATERLINE, BEING THE WATERS EDGE OF MILL COVE; THENCE SOUTHWESTERLY, MEANDERING ALONG SAID WATERS EDGE 2,325 FEET MORE OR LESS TO AN INTERSECTION WITH THE WESTERLY LINE OF A 300' SEA EASEMENT; THENCE NORTH 15°15'34" WEST, ALONG SAID WESTERLY LINE 2,655 FEET MORE OR LESS TO THE MEAN HIGH WATERLINE, BEING THE WATERS EDGE OF THE ST. JOHNS RIVER; THENCE NORTHEASTERLY ALONG SAID WATERS EDGE 1,290 FEET MORE OR LESS, THENCE SOUTH 00°01'51" EAST, DEPARTING SAID WATERS EDGE, 198 FEET MORE OR LESS TO A POINT OF CURVATURE OF A CURVE CONCAVE NORTHEASTERLY, HAVING A RADIUS OF 135.00 FEET, THENCE SOUTHEASTERLY, ALONG AND AROUND THE ARC OF SAID CURVE A DISTANCE OF 212.06 FEET, THROUGH A CENTRAL ANGLE OF 90°00'00"; AND BEING SUBTENDED BY A CHORD BEARING AND DISTANCE OF SOUTH 45°01'51" EAST, 130.92 FEET TO THE POINT OF TANGENCY OF SAID CURVE; THENCE NORTH 89°58'09" EAST, 360.00 FEET; THENCE SOUTH 00°01'52" EAST, 1,547.39 FEET TO THE POINT OF BEGINNING.

CONTAINING 79.07 ACRES (3,444,429 SQUARE FEET), MORE OR LESS.

TOGETHER WITH THE FOLLOWING DESCRIBED PARCEL:

PARCEL B

A PORTION OF SECTION 31, TOWNSHIP 1 SOUTH, RANGE 28 EAST, DUVAL COUNTY, FLORIDA, BEING MORE PARTICULARLY DESCRIBED AS FOLLOWS:

AN ISLAND LYING SOUTHERLY OF PARCEL A DESCRIBED HERE ON, LYING IN MILL COVE AND RUNNING ALONG THE MEAN HIGH WATER LINE, BEING THE WATERS EDGE FOR A TOTAL PERIMETER DISTANCE OF 2,288 FEET MORE OR LESS.

CONTAINING 3.14 ACRES (135,610 SQUARE FEET), MORE OR LESS.

ALL ABOVE CONTAINING 82.21 ACRES (3,581,039 SQUARE FEET), MORE OR LESS.

SURVEY NOTES

NOTE: THIS MAP DOES NOT REPRESENT A BOUNDARY SURVEY.

- 1 BEARINGS SHOWN HEREON ARE BASED ON THE SOUTHERLY LINE OF SECTION 30 AS BEING N 89°15'09" W (PER PLAT)
- 2 ALL DIMENSIONS SHOWN HEREON ARE IN FEET AND IN TENTHS AND ARE BASED ON THE U.S. SURVEY FOOT
- 3 A TITLE COMMITMENT HAS NOT BEEN PROVIDED
- 4 NOTICE: THERE MAY BE ADDITIONAL RESTRICTIONS THAT ARE NOT SHOWN ON THIS SURVEY THAT MAY BE FOUND IN THE PUBLIC RECORDS OF THIS COUNTY.

SEE SHEET 2 FOR SKETCH
SHEET 1 OF 2

JOHN K. MAFFETT
Florida Registration Certificate No. 0951
NOT VALID WITHOUT THE SIGNATURE AND
THE ORIGINAL RAISED SEAL OF A FLORIDA
LICENSED SURVEYOR AND MAPPER

ARC SURVEYING & MAPPING, INC.



5202 SAN JUAN AVENUE,
JACKSONVILLE, FLORIDA 32210
PHONE 904/384-8377
LICENSED BUSINESS NO. 6487

DRAWN BY:	DATE:	FIELD BOOK & PAGE	JOB NO.
JK4	10-11-22	--	22-223

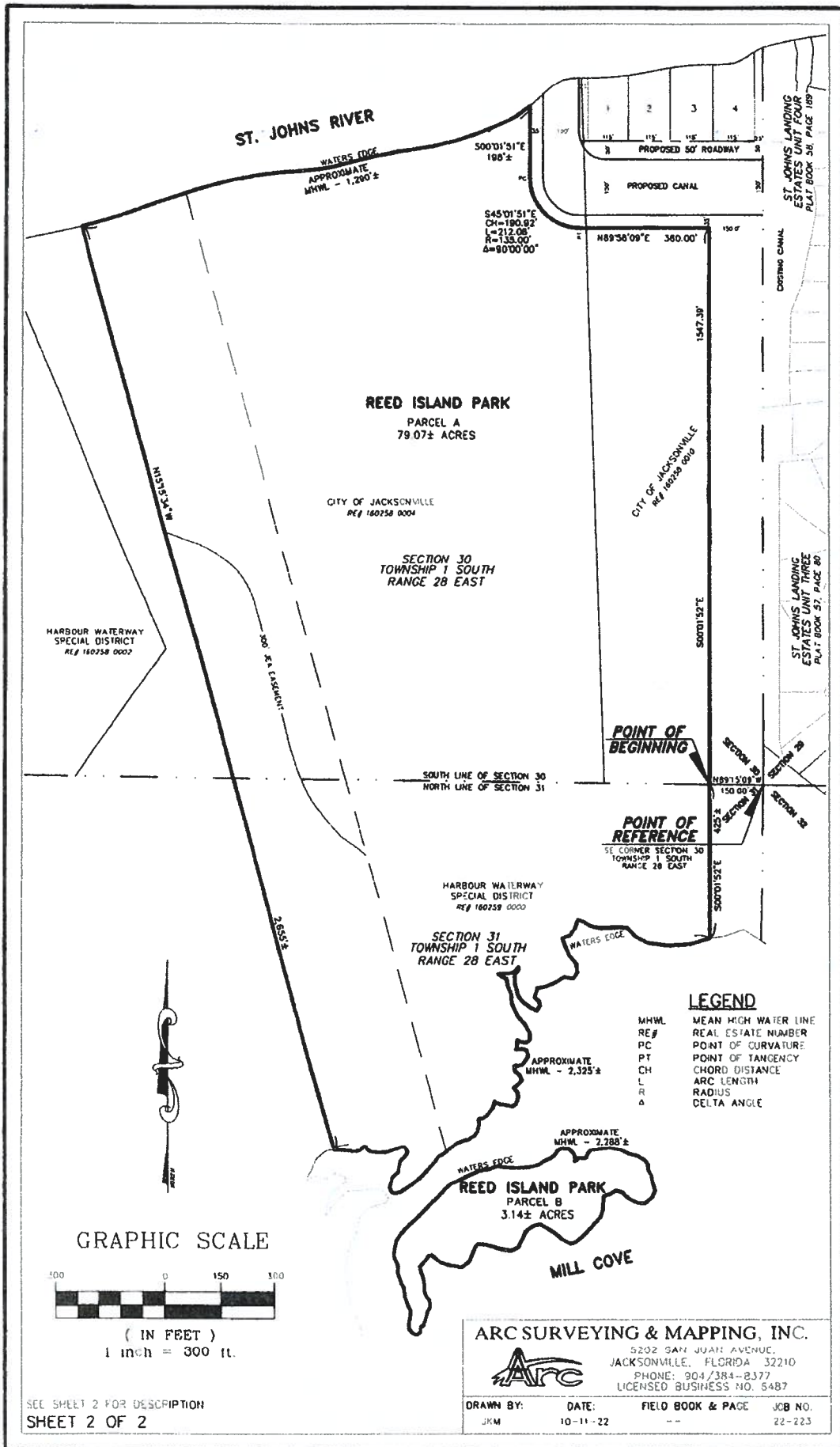


Exhibit "C"
page 1 of 2





Exhibit "D"
Page 1 of 2

PROSSER
 Civil/Structural/Engineering/Architecture
 1100 South Orange Avenue, Suite 200
 Jacksonville, Florida 32209
 Phone: 904.775.1000
 Fax: 904.775.1001

Professional Seal

CITY OF
 JACKSONVILLE

REED ISLAND
 COURTESY DOCKS

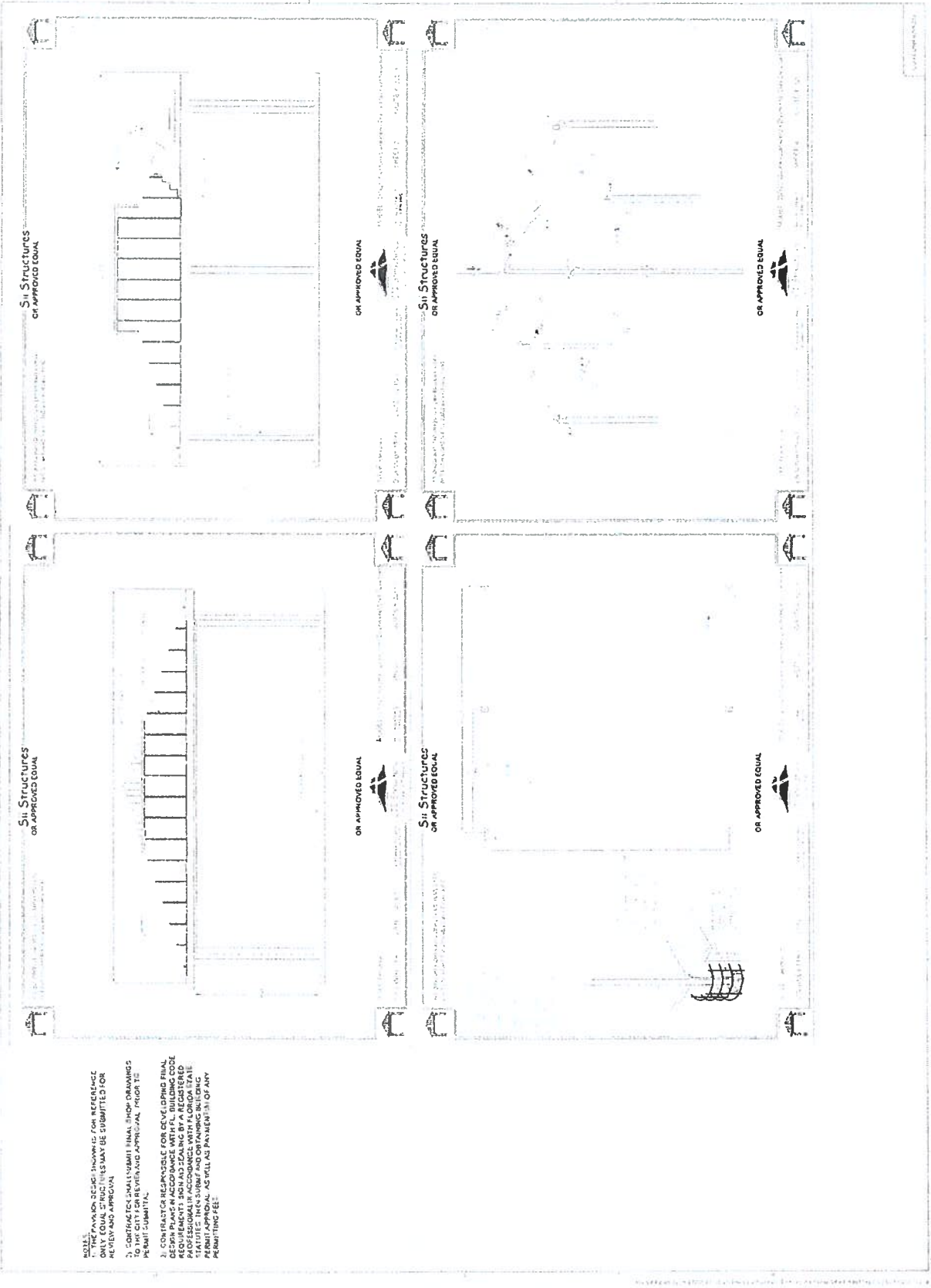
PARKS, RECREATION
 AND COMMUNITY
 SERVICE



NO.	DATE	DESCRIPTION
1	08/11/11	ISSUED FOR PERMITS
2	08/11/11	ISSUED FOR PERMITS
3	08/11/11	ISSUED FOR PERMITS
4	08/11/11	ISSUED FOR PERMITS
5	08/11/11	ISSUED FOR PERMITS
6	08/11/11	ISSUED FOR PERMITS
7	08/11/11	ISSUED FOR PERMITS
8	08/11/11	ISSUED FOR PERMITS
9	08/11/11	ISSUED FOR PERMITS
10	08/11/11	ISSUED FOR PERMITS
11	08/11/11	ISSUED FOR PERMITS
12	08/11/11	ISSUED FOR PERMITS
13	08/11/11	ISSUED FOR PERMITS
14	08/11/11	ISSUED FOR PERMITS
15	08/11/11	ISSUED FOR PERMITS
16	08/11/11	ISSUED FOR PERMITS
17	08/11/11	ISSUED FOR PERMITS
18	08/11/11	ISSUED FOR PERMITS
19	08/11/11	ISSUED FOR PERMITS
20	08/11/11	ISSUED FOR PERMITS

SITE DETAILS

L5 01
 SHEET NO. 1501
 OF 1501



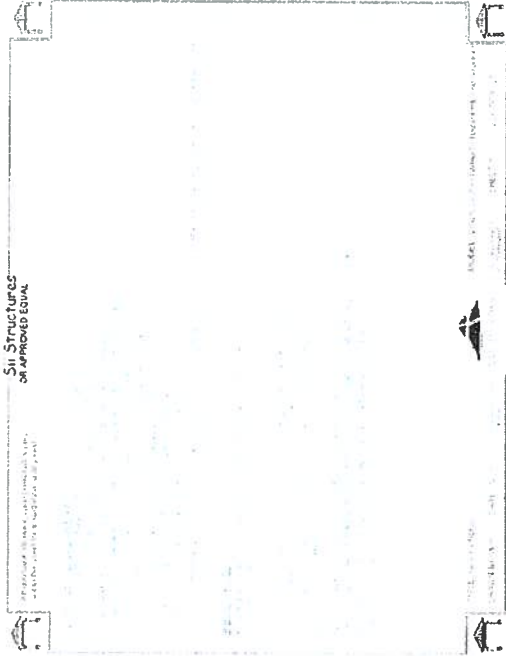
NOTES:
 1. THE FOLLOWING SEALS ARE REQUIRED FOR PERMITS:
 ARCHITECTURAL SEALS MAY BE SUBMITTED FOR
 REVIEW AND APPROVAL.
 2. CONTRACTORS SHALL SUBMIT FINAL ARCHITECTURAL DRAWINGS
 TO THE CITY FOR REVIEW AND APPROVAL PRIOR TO
 PERMIT SUBMITTAL.
 3. CONTRACTORS RESPONSIBLE FOR OBTAINING FINAL
 DESIGN PLANS IN ACCORDANCE WITH ALL BUILDING CODE
 REQUIREMENTS AND SEALING BY A REGISTERED
 ARCHITECT. CONTRACTORS SHALL SUBMIT AND OBTAIN THE
 PERMIT APPROVAL AS WELL AS PAYMENT OF ANY
 PERMITTING FEE.

Exhibit 09
Page 2 of 2

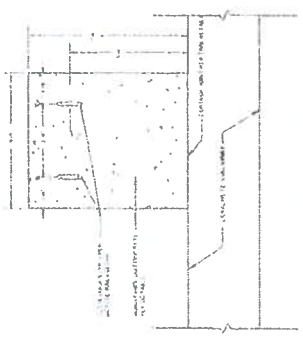
PARK EQUIPMENT NOTES:

1. GRILL - ACCESSIBLE PEDESTAL GRILL WITH SWING OUT COOKING GRATE MODEL FSM-18 ACCESSIBLE BY NAY PARK RECREATION CORP. OR APPROVED EQUAL. MOUNT & INSTALL PER MANUFACTURER'S RECOMMENDATIONS. QUANTITY (2) TWO TOTAL
2. PICNIC TABLE - WHEELCHAIR ACCESSIBLE PICNIC TABLE. 8FT LONG 40" W/4" BLUE END COLOR AND 8FT LONG SEATS CEDAR/BROWN COLOR BY BRIGHTIDEAWORKS.COM OR APPROVED EQUAL. QUANTITY (6) SIX TOTAL
3. PAVILION - 25' X 25' CUSTOM LAMINATED DUTCH HOP END STRUCTURE BY JJI STRUCTURES OR APPROVED EQUAL. SEE SHEETS L5.01 & L5.02. QUANTITY (2) TWO TOTAL

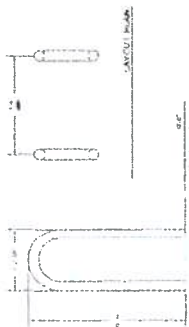
Site Structures
SH APPROVED EQUAL



NOTES:
1) SEE NOTES SHEETS L5.01



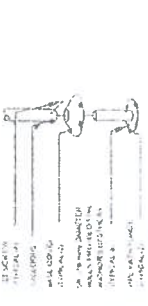
BICYCLE RACK DETAIL



PICNIC TABLE DETAIL



GRILL DETAIL



PICNIC TABLE WITH BENCH DETAIL

COLUMBIA PACAGE COMPANY
1000 N. 10TH ST. SUITE 100
DENVER, CO 80202
TEL: 303.733.1111
WWW.COLUMBIAPACAGE.COM

BICYCLE RACK DETAIL



PROSSER
Engineering Inc.
11411 1/2 W. 10th Ave., Suite 200
Golden, CO 80401
303.733.1111

CITY OF JACKSONVILLE

REED ISLAND COURTESY DOCKS

PARKS, RECREATION AND COMMUNITY SERVICE



NO.	DATE	DESCRIPTION
1	08/20/2012	ISSUED FOR PERMIT
2	08/20/2012	ISSUED FOR PERMIT
3	08/20/2012	ISSUED FOR PERMIT
4	08/20/2012	ISSUED FOR PERMIT
5	08/20/2012	ISSUED FOR PERMIT
6	08/20/2012	ISSUED FOR PERMIT
7	08/20/2012	ISSUED FOR PERMIT
8	08/20/2012	ISSUED FOR PERMIT
9	08/20/2012	ISSUED FOR PERMIT
10	08/20/2012	ISSUED FOR PERMIT

NO.	DATE	DESCRIPTION
1	08/20/2012	ISSUED FOR PERMIT
2	08/20/2012	ISSUED FOR PERMIT
3	08/20/2012	ISSUED FOR PERMIT
4	08/20/2012	ISSUED FOR PERMIT
5	08/20/2012	ISSUED FOR PERMIT
6	08/20/2012	ISSUED FOR PERMIT
7	08/20/2012	ISSUED FOR PERMIT
8	08/20/2012	ISSUED FOR PERMIT
9	08/20/2012	ISSUED FOR PERMIT
10	08/20/2012	ISSUED FOR PERMIT

SITE DETAILS

L5.02
15.02
3 OF 11

RESOLUTION NO. 2023-08

**A RESOLUTION OF THE HARBOUR WATERWAY SPECIAL DISTRICT,
DUVAL COUNTY, FLORIDA, ADOPTING THE HARBOUR WATERWAY
SPECIAL DISTRICT INFORMATION SECURITY POLICY; PROVIDING
AN EFFECTIVE DATE.**

WHEREAS, the Harbour Waterway Special District (“HWSD”), was established through City of Jacksonville Ordinance No. 2010-725-E (“Ordinance”) and given responsibility therein for maintenance of the system of canals located within the boundaries of the HWSD ; and

WHEREAS, the Board of Supervisors (“Board”) of the HWSD has determined that adoption of an Information Security Policy to provide direction and guidance to the Board regarding the handling of confidential information to be followed in conducting its business would be beneficial for the Board and for residents of the HWSD.

NOW THEREFORE, BE IT RESOLVED by the Board of the HWSD:

Section 1. The Board hereby adopts the Information Security Policy attached hereto as Exhibit “A” , to be utilized by the Board in the conduct of HWSD business.

Section 3. This Resolution shall become effective upon adoption.

Passed and Adopted this 11th day of July, 2023.



Wallace G. Lovely
Board Chair

Attest:



Robert P. Birtalan
Board Secretary

Information Security Policy

Harbour Waterway Special District

June 1, 2023

Contents

1. Introduction	3
2. Information Security Policy	3
3. Acceptable Use Policy	4
4. Disciplinary Action.....	4
5. Protect Stored Data	4
6. Information Classification	5
7. Access to the sensitive cardholder data	5
8. Physical Security.....	6
9. Protect Data in Transit	7
10. Disposal of Stored Data.....	8
11. Security Awareness and Procedures.....	8
12. Network security	9
13. System and Password Policy.....	10
14. Anti-virus policy	11
15. Patch Management Policy	11
16. Remote Access policy.....	12
17. Vulnerability Management Policy.....	12
18. Configuration standards:	12
19. Change control Process.....	13
20. Audit and Log review	14
21. Secure Application development.....	17
22. Penetration testing methodology.....	18
23. Incident Response Plan	20
24. Roles and Responsibilities.....	24
25. Third party access to card holder data	25
26. User Access Management.....	25
27. Access Control Policy	26
28. Wireless Policy	27
Appendix A.....	29
Appendix B	30

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential District information and must be distributed to all District employees. All District employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

Harbour Waterway Special District (HWSD) handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

HWSD commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure:

- Handle District and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of **HWSD** information and telecommunication systems and ensure it doesn't interfere with your job performance;
- **HWSD** reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other District resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our District's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to **HWSD's** established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and **HWSD** from illegal or damaging actions by individuals, either knowingly or unknowingly. **HWSD** will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a District email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of **HWSD**, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non compliance.

5. Protect Stored Data

- All sensitive cardholder data stored and handled by **HWSD** and its employees must be securely protected against unauthorized use at all times. Any sensitive card data that is no longer required by **HWSD** for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to **HWSD** if disclosed or modified. **Confidential data includes cardholder data.**
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7. Access to the sensitive cardholder data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- **HWSD** will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- **HWSD** will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- **HWSD** will have a process in place to monitor the PCI DSS compliance status of the Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on **HWSD** sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver

enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by **HWSD**, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- **HWSD** will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- **HWSD** will have documented procedures for the destruction of electronic media. These will require:
 - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
 - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into District practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day District practice.
- Distribute this security policy document to all District employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with **HWSD**.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- District security policies must be reviewed annually and updated as needed.

12. Network security

- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal District network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- Stateful Firewall technology must be implemented where the Internet enters **HWSD** Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented
- **HWSD** will have firewalls between any wireless networks and the cardholder data environment.
- **HWSD** will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- **HWSD** have to quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet.
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

Rules	Source IP	Destination IP	Action

--	--	--	--

13. System and Password Policy

All users, including contractors and vendors with access to **HWSD** systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO)
- System configurations should be updated as new issues are identified (as defined in PCI DSS requirement 6.1)
- System configurations must include common security parameter settings
- The systems configuration standard should be applied to any news systems configured.
- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into **HWSD** network and all unnecessary services and user/system accounts have to be disabled.
- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must me set appropriately on System components
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified.
- All users with access to card holder data must have a unique ID.
- All user must use a password to access **HWSD** network or any other electronic resources
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All system and user level passwords must be changed on at least a quarterly basis.
- A minimum password history of four must be implemented.
- A unique password must be setup for new users and the users prompted to change the password on first login.
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All non-console administrative access will use appropriate technologies like ssh,vpn etc or strong encryption is invoked before the administrator password is requested
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands
- Administrator access to web based management interfaces is encrypted using strong cryptography.
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

- a) Be as long as possible (never shorter than 6 characters).
 - b) Include mixed-case letters, if possible.
 - c) Include digits and punctuation marks, if possible.
 - d) Not be based on any personal information.
 - e) Not be based on any dictionary word, in any language.
- If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
 - To protect against network analysis attacks, both the workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

14. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by **HWSD**. The preferred application to use is **McAfee** Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- End users must not be able to modify any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

15. Patch Management Policy

- All Workstations, servers, software, system components etc. owned by **HWSD** must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.
- Any exceptions to this process have to be documented.

16. Remote Access policy

- It is the responsibility of **HWSD** employees, contractors, vendors and agents with remote access privileges to **HWSD**'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to **HWSD**.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
- Vendor accounts with access to **HWSD** network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity
- All hosts that are connected to **HWSD** internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or 3rd parties will be reconciled at regular intervals and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to **HWSD** network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

17. Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
- As part of the PCI-DSS Compliance requirements, **HWSD** will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by **HWSD** by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by **HWSD**'s internal staff. The scan process should include re-scans until passing results are obtained.

18. Configuration standards:

- Information systems that process transmit, or store card holder data must be configured in accordance with the applicable standard for that class of device or system. Standards must be written and maintained by the team responsible for the management of the system in conjunction with the Information Security Office.
- All network device configurations must adhere to **HWSD** required standards before being placed on the network as specified in **HWSD** configuration guide. Using this guide, a boilerplate

configuration has been created that will be applied to all network devices before being placed on the network.

- Before being deployed into production, a system must be certified to meet the applicable configuration standard
- Updates to network device operating system and/or configuration settings that fall under **HWSD** standards are announced by the Information security Office. Updates must be applied within the time frame identified by the Information security Office.
- Administrators of network devices that do not adhere to **HWSD** standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.
- All network device configurations must be checked annually against the configuration boilerplate to ensure the configuration continues to meet required standards.
- Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.
- For other devices an audit will be performed quarterly to compare the boilerplate configuration to the configuration currently in place.
- All discrepancies will be evaluated and remediated by Network Administration.

19. Change control Process

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical District information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.
- All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.
- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. (For more information see System Development Life Cycle).
- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies. (For more information see System Development Life Cycle)
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.
- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see System Development Life Cycle)
- Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.
- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

20. Audit and Log review

- This procedure covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over **HWSD** network, including the following components:

- Operating System Logs (Event Logs and su logs).
 - Database Audit Logs.
 - Firewalls & Network Switch Logs.
 - IDS Logs.
 - Antivirus Logs.
 - Cctv Video recordings.
 - File integrity monitoring system logs.
- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
 - Review of logs is to be carried out by means of **HWSD's** network monitoring system (**HWSD** to define hostname), which is controlled from **HWSD** console (**HWSD** to define hostname). The console is installed on the server (**HWSD** to define hostname / IP address), located within **HWSD** data centre environment.
 - The following personnel are the only people permitted to access log files (**HWSD** to define which individuals have a job-related need to view audit trails and access log files).
 - The network monitoring system software (**HWSD** to define) is configured to alert **HWSD's** District Manager to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to:
 - A dashboard browser-based interface, monitored by **HWSD's** District Manager.
 - Email / SMS alerts to **HWSD's** mailbox with a summary of the incident. **HWSD's** District Manager also receives details of email alerts for informational purposes.
 - The following Operating System Events are configured for logging, and are monitored by the console:
 - a) Any additions, modifications or deletions of user accounts.
 - b) Any failed or unauthorised attempt at user logon.
 - c) Any modification to system files.
 - d) Any access to the server, or application running on the server, including files that hold cardholder data.
 - e) Actions taken by any individual with root or administrative privileges.
 - f) Any user access to audit trails.
 - g) Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)
 - The following Database System Events are configured for logging, and are monitored by the network monitoring system (if applicable):
 - a) Any failed user access attempts to log in to the Oracle database.
 - b) Any login that has been added or removed as a database user to a database.
 - c) Any login that has been added or removed from a role.
 - d) Any database role that has been added or removed from a database.
 - e) Any password that has been changed for an application role.
 - f) Any database that has been created, altered, or dropped.
 - g) Any database object, such as a schema, that has been connected to.
 - h) Actions taken by any individual with DBA privileges.

- The following Firewall Events are configured for logging, and are monitored by the network monitoring system (if applicable):
 - a) ACL violations.
 - b) Invalid user authentication attempts.
 - c) Logon and actions taken by any individual using privileged accounts.
 - d) Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).

- The following Switch Events are to be configured for logging and monitored by the network monitoring system (if applicable):
 - a) Invalid user authentication attempts.
 - b) Logon and actions taken by any individual using privileged accounts.
 - c) Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified).

- The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (if applicable):
 - a) Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
 - b) Any generic attack(s) not listed in CVE.
 - c) Any known denial of service attack(s).
 - d) Any traffic patterns that indicated pre-attack reconnaissance occurred.
 - e) Any attempts to exploit security-related configuration errors.
 - f) Any authentication failure(s) that might indicate an attack.
 - g) Any traffic to or from a back-door program.
 - h) Any traffic typical of known stealth attacks.

- The following File Integrity Events are to be configured for logging and monitored (if applicable):
 - a) Any modification to system files.
 - b) Actions taken by any individual with Administrative privileges.
 - c) Any user access to audit trails.
 - d) Any Creation / Deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

- For any suspicious event confirmed, the following must be recorded on F17 - Log Review Form, and **HWSD's** District Manager informed:
 - a) User Identification.
 - b) Event Type.
 - c) Date & Time.
 - d) Success or Failure indication.
 - e) Event Origination (e.g. IP address).
 - f) Reference to the data, system component or resource affected.

21. Secure Application development

- The Secure Application development policy is a plan of action to guide developers' decisions and actions during the software development lifecycle (SDLC) to ensure software security. This policy aims to be language and platform independent so that it is applicable across all software development projects.
- The adherence to and use of Secure Application Development Coding Policy is a requirement for all software development on **HWSD** information technology systems and trusted contractor sites processing **HWSD** data.
- Each phase of the SDLC is mapped with security activities, as explained below:
 - a) Design
 - Identify Design Requirements from security perspective
 - Architecture & Design Reviews
 - Threat Modelling
 - b) Coding
 - Coding Best Practices
 - Perform Static Analysis
 - c) Testing
 - Vulnerability Assessment
 - Fuzzing
 - d) Deployment
 - Server Configuration Review
 - Network Configuration Review
- Development of code shall be checked and validated with the most current versions of **HWSD** Coding Standards for Secure Application Development. All code developers shall verify that their code is in compliance with the most recent and approved coding standards and guidelines.
- Only validated code shall be implemented into **HWSD** production environment. A review and validation ensures that code exhibits fundamental security properties to include correctness, predictability, and attack tolerance.

Application Code Developers shall:

- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.
- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended.
- Coding techniques must address injection flaws particularly SQL injection, buffer overflow vulnerabilities, cross site scripting vulnerabilities, improper access control (insecure direct object

reference, failure to restrict URL access, directory traversal etc.), cross site request forgery (CSRF), broken authentication and session management

- Never trust incoming data to the system, apply checks to this data.
- Never rely on the client to store sensitive data no matter how trivial.
- Disable Error messages that return any information to the user.
- Use object inheritance, encapsulation, and polymorphism wherever possible.
- Use environment variables prudently and always check boundaries and buffers.
- Applications must validate input to ensure it is well-formed and meaningful.

22. Penetration testing methodology

- In this section should be listed the risks inherent in conducting penetration testing over the information systems of **HWSD**. Additionally, it should be noted for each mitigation measures that will be taken. Examples might be:

Example 1#

Risk: Denial of Service in systems or network devices because of the network scans.

Mitigation measure 1: network scans must be performed in a controlled manner. The start and end of the scan must be notified to responsible personnel to allow monitoring during testing. For any sign of trouble will abort the scan in progress.

Mitigation measure 2: scanning tools must be configured to guarantee that the volume of sent packets or sessions established per minute does not cause a problem for network elements. In this sense, we must perform the first scans in a very controlled way and a use minimum configuration that may be expanded when is evident that the configuration is not dangerous for network devices or servers in the organization.

- Key staff involved in the project by the organization will be listed:

Technical Project Manager:

Chief Information Security Officer:

Chief Information Officer:

Head of Communications:

Responsible for web site **HWSD.org**:

- External intrusion tests will be performed remotely from the supplier's premises. Internal intrusion tests will be conducted in the **HWSD** office of the Organization. Audit team must to have access to the Organization's network. It must manage access permissions to the building early enough to ensure that the audit team can access without problems during planning period.
- All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.

- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organization, the incident should be brought immediately to the attention of those responsible for incident management in the project
- It should be noted that in order to comply with PCI DSS the scope of the test should include, at least the following:
 - All systems and applications that are part of the perimeter of the cardholder data environment card (CDE).

Example:

a) Systems included in the scope

System 1: IP: System: System Description

System 2: IP: System: System Description

Wifi network **HWSD**

.....

b) Applications included in the scope

Application 1: URL: Description of the application

.....

c) Systems excluded from the scope

System 5: IP: System: System Description

System 6: IP: System: System Description

.....

d) Applications excluded from the scope

Application 3: URL: Description of the application

.....

- Technical tests must follow the OSSTMM methodology. Tests must be conducted at network, system and application level and must ensure that at least identifies any vulnerabilities documented by OWASP and SANS, as well as those identified in the PCI DSS standard v3:
 1. Injections: Code, SQL, OS commands, LDAP , XPath , etc.
 2. Buffer overflows.
 3. Insecure storage of cryptographic keys
 4. Insecure Communications
 5. Improper error handling
 6. Cross -site scripting (XSS)
 7. Control of inappropriate access.
 8. Cross - site request forgery (CSRF).
 9. Broken authentication and incorrectly session management.
 10. Any other vulnerability considered High Risk by the organization.
- For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence

can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.

- As a result of tests performed should generate a document containing at least the following sections:

Introduction
Executive Summary
Methodology
Identified vulnerabilities
Recommendations for correcting vulnerabilities
Conclusions
Evidence

23. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your District.

The Incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Employees of **HWSD** will be expected to report to the security officer for any security related issues.

HWSD PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. That member of the team receiving the report will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
6. If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Security officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.
7. A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform **HWSD** PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along

with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

HWSD PCI Security Incident Response Team:

CIO

Communications Director

Compliance Officer

Counsel

Information Security Officer

Collections & Merchant Services

Risk Manager

Incident Response Notification

Escalation Members

Escalation – First Level

Information Security Officer

Controller

Executive Project Director for Credit Collections and Merchant Services Legal

Counsel

Risk Manager

Director of **HWSD** Communications

Escalation – Second Level

HWSD Chairman

Executive Cabinet

Internal Audit

Auxiliary members as needed

External Contacts (as needed)

Merchant Provider Card

Brands

Internet Service Provider (if applicable)

Internet Service Provider of Intruder (if applicable)

Communication Carriers (local and long distance) Business

Partners

Insurance Carrier

External Response Team as applicable (CERT Coordination Center 1, etc) Law

Enforcement Agencies as applicable in local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.

5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (Truist Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit:
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

- I. Executive Summary
 - a. Include overview of the incident
 - b. Include RISK Level (High, Medium, Low)
 - c. Determine if compromise has been contained
- II. Background
- III. Initial Analysis
- IV. Investigative Procedures
 - a. Include forensic tools used during investigation
- V. Findings
 - a. Number of accounts at risk, identify those stores and compromised
 - b. Type of account information at risk

- c. Identify ALL systems analyzed. Include the following:
 - Domain Name System (DNS) names
 - Internet Protocol (IP) addresses
 - Operating System (OS) version
 - Function of system(s)
- d. Identify ALL compromised systems. Include the following:
 - DNS names
 - IP addresses
 - OS version
 - Function of System(s)
- e. Timeframe of compromise
- f. Any data exported by intruder
- g. Establish how and source of compromise
- h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
- i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

Employees of **HWSD** will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within **HWSD** and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
4. Obtain additional specific requirements from Discover Card

American Express Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
Obtain additional specific requirements from American Express

24. Roles and Responsibilities

- Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:
 - Creating and distributing security policies and procedures.
 - Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
 - creating and distributing security incident response and escalation procedures that include:
 - Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
- The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).
- System and Application Administrators shall:
 - monitor and analyse security alerts and information and distribute to appropriate personnel

- administer user accounts and manage authentication
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.
- The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:
 - Facilitating participation upon hire and at least annually.
 - Ensuring that employees acknowledge in writing at least annually that they have read and understand **HWSD's** information security policy.
- General Counsel (or equivalent) will ensure that for service providers with whom cardholder information is shared:
 - Written contracts require adherence to PCI-DSS by the service provider.
 - Written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.

25. Third party access to card holder data

- All third-party companies providing critical services to **HWSD** must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with **HWSD's** Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:
 1. Adhere to the PCI DSS security requirements.
 2. Acknowledge their responsibility for securing the Card Holder data.
 3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
 4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
 5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

26. User Access Management

- Access to **HWSD** is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.

- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

Name of person making request:

Job title of the newcomers and workgroup:

Start date:

Services required (default services are: MS Outlook, MS Office and Internet access):

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all **HWSD** systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves **HWSD** employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

27. Access Control Policy

- Access Control systems are in place to protect the interests of all users of **HWSD** computer systems by providing a safe, secure and readily accessible environment in which to work.
- **HWSD** will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification
- Users are obligated to report instances of non-compliance to the **HWSD** CISO
- Access to **HWSD** IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any **HWSD** IT resources and services will be provided without prior authentication and authorization of a user's **HWSD** Windows Active Directory account.

- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by **HWSD** policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights

28. Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the **HWSD** networks or environments is prohibited.
- A quarterly test should be run to discover any wireless access points connected to **HWSD** network
- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
 - Any devices which support wireless communication remain disabled or decommissioned.
 - If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the security officer or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology it should be approved by **HWSD** and the following wireless standards have to be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves **HWSD**.

2. The firmware on the wireless devices has to be updated accordingly as per vendors release schedule
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.
6. An Inventory of authorized access points along with a business justification must be maintained. (Update Appendix B)

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

Employee Name (printed)

Department

I agree to take all reasonable precautions to assure that District internal information, or information that has been entrusted to **HWSD** by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with **HWSD**, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in **HWSD** security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

Employee Signature

Appendix B

DvhwGhy'fhn@dp h# #	Ghvfuswrq# #	Rz qhUssuryhg#Kvh# #	Orfdwrq# #
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#
#	#	#	#

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date

**HARBOUR WATERWAY SPECIAL DISTRICT
RESOLUTION NO. 2023 - 07**

**A RESOLUTION OF THE HARBOUR WATERWAY SPECIAL DISTRICT,
DUVAL COUNTY, FLORIDA, ADOPTING A NON-AD VALOREM
ASSESSMENT ROLL FOR 2023 AND LEVYING NON-AD VALOREM
ASSESSMENTS ON LOTS AND PARCELS IN THE DISTRICT;
PROVIDING AN EFFECTIVE DATE.**

WHEREAS, on February 7, 2012, the Board of Supervisors (“Board”) of the Harbour Waterway Special District (“HWSD”) approved a duly noticed Resolution adopting the Uniform Method for Collecting Non-Ad Valorem Assessments, in conformance with Section 197.3632, Florida Statutes; and

WHEREAS, on June 8, 2023, a notice was published in a newspaper of general circulation in Duval County, Florida, giving notice of the date, time and location at which a public hearing would be conducted to consider adoption of a Resolution approving the non-ad valorem Roll for the HWSD as well as imposing non-ad valorem assessments on the lots and parcels in the HWSD for fiscal year 2023-2024; and

WHEREAS, a public hearing was conducted on this date, consistent with the notice provided by publication, at which testimony was received by the Board of Supervisors for the HWSD (“Board”) regarding the proposed non-ad valorem assessments on lots and parcels in the HWSD; and

WHEREAS, the Board finds that the purpose of the non-ad valorem assessments approved through this Resolution is to provide funds for conducting maintenance dredging of the system of canals located in the HWSD and to dispose of the dredged material removed from the canal system in connection with the maintenance dredging, and provide access to the canal system by maintaining a marina on the waterway a purpose consistent with the authority given to the HWSD in City of Jacksonville Ordinance No. 2010-725-E; and

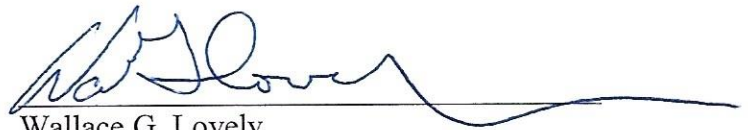
WHEREAS, the Board finds that the non-ad valorem assessments approved through this Resolution will benefit all properties assessed as a consequence of the maintenance dredging project and further finds that the non-ad valorem assessment approved through this Resolution is fairly and equitably apportioned among the properties receiving the benefit of the maintenance dredging project to be funded through the assessment.

NOW THEREFORE, Be it Resolved by the Board of the HWSD that:


Section 1. The Non-Ad Valorem Assessment Roll attached hereto as Exhibit "A" is hereby certified and the assessments specified thereon are adopted for the lots and parcels listed thereon for Fiscal Year 2023-2024.

Section 2. This Resolution shall become effective upon adoption.

Passed and Adopted this 11th day of July, 2023.


Wallace G. Lovely
Board Chair

Attest:


Robert P. Birtalan
Board Secretary / Treasurer

**HARBOUR WATERWAY SPECIAL DISTRICT
PROPOSED 2023 NON-AD VALOREM ASSESSMENT**

CDD/SD CODE	STRAP	OWNER	ADDRESS	PARCEL LOCATION				NON-AD VALOREM ASSESSMENT
				STREET	CITY	ST	ZIP	
HWSD1	R-160258-0002	HARBOUR WATERWAY SPECIAL DISTRICT	0	ASHLEY MANOR WAY	JACKSONVILLE	FL	32225	0.00
HWSD1	R-160259-0000	HARBOUR WATERWAY SPECIAL DISTRICT	0	ASHLEY MANOR WAY	JACKSONVILLE	FL	32225	0.00
HWSD1	R-160266-1150	HARBOUR WATERWAY SPECIAL DISTRICT	4639	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	0.00
HWSD1	R-160266-0900	HARBOUR WATERWAY SPECIAL DISTRICT	0	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	0.00
HWSD1	R-160671-0080	HARBOUR WATERWAY SPECIAL DISTRICT	0	HARBOUR WOODS DR	JACKSONVILLE	FL	32225	0.00
HWSD1	R-160264-0000	DYNAMIC HOMES OF NE FLORIDA INC	0	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-6519	500.00
HWSD1	R-160265-0000	GEBREMEDHIN TIRHAS BERHANE	0	HARBOUR NORTH CT	JACKSONVILLE	FL	32244	2,000.00
HWSD1	R-160265-0025	BONEY WALTER T ET AL	0	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-	500.00
HWSD1	R-160265-1005	WHITE MILDRED G	11026	HARBOR CAY CT	JACKSONVILLE	FL	32225-4043	2,000.00
HWSD1	R-160266-0000	LARRY DEAN TRUSTEE	0	HARBOUR WOODS DR	JACKSONVILLE	FL	32247-8070	2,000.00
HWSD1	R-160266-1040	PINARD CHRISTOPHER C	4595	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1078	0.00
HWSD1	R-160266-1160	PADGETT DON G J	11066	HARBOR CAY CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-1180	DRACIC ANES	11050	HARBOR CAY CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-1200	BROCK LINDSEY C III	11042	HARBOR CAY CT	JACKSONVILLE	FL	32225-4043	2,000.00
HWSD1	R-160266-2008	SHAEFFER WILLETTE	4206	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160266-2016	BINGHAM ROBERT	4230	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160266-2020	DAVIS GLENN R	4308	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1564	750.00
HWSD1	R-160266-2023	WALTON MELISSA R	0	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-6519	500.00
HWSD1	R-160266-2024	WILLIAMS JUDD ET AL	4322	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160266-2025	REGAN DAVID M	4330	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1564	750.00
HWSD1	R-160266-2026	LAND TRUST #160266-2026	0	HARBOUR ISLAND DR	JACKSONVILLE	FL	32247	500.00
HWSD1	R-160266-2027	RNAA LLC	0	HARBOUR ISLAND DR	JACKSONVILLE	FL	32256	500.00
HWSD1	R-160266-2028	LE NHUT T	4459	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1555	2,000.00
HWSD1	R-160266-2029	STALLINGS TOM C JR	0	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160266-2030	LE NHUT TUAN	4453	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1555	2,000.00
HWSD1	R-160266-2032	HUMPHREYS MARK D	4447	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2034	BURDIAN STEPHEN V	4439	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2036	CRUZ ANTHONY ALBERT	4431	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1567	2,000.00
HWSD1	R-160266-2038	PALMER TIMOTHY A	4425	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2040	BRANDENBURG BETTY M ET AL	4419	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1567	2,000.00
HWSD1	R-160266-2042	CAUDLE AUBREY B	4413	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2044	TODD MARK E	4407	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1567	2,000.00
HWSD1	R-160266-2046	HOLDER MARK DANIEL	4343	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2048	LUEDERS LIVING TRUST	4337	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1565	2,000.00

**HARBOUR WATERWAY SPECIAL DISTRICT
PROPOSED 2023 NON-AD VALOREM ASSESSMENT**

CDD/SD CODE	STRAP	OWNER	PARCEL LOCATION					NON-AD VALOREM ASSESSMENT
			ADDRESS	STREET	CITY	ST	ZIP	
HWSD1	R-160266-2050	WHITE JAMES A	4331	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1565	2,000.00
HWSD1	R-160266-2052	JONES AMANDA N	4325	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2054	GIBBS ROBERT KINGSLEY JR	4317	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2055	ERIKSEN ANDREW BLAKE	4311	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2057	EDWARDS SANJAE E	4305	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1565	1,000.00
HWSD1	R-160266-2060	FERRARO ALBERT J JR	11187	SCHOONER CT	JACKSONVILLE	FL	32225-1561	2,000.00
HWSD1	R-160266-2062	BIRTALAN ROBERT P	11191	SCHOONER CT	JACKSONVILLE	FL	32225-1561	2,000.00
HWSD1	R-160266-2064	DORIS MARK J	11194	SCHOONER CT	JACKSONVILLE	FL	32225-1561	2,000.00
HWSD1	R-160266-2066	JONES MICHAEL P	11188	SCHOONER CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2068	VONGSAY THONGPHAT ET AL	4229	HARBOUR ISLAND DR	JACKSONVILLE	FL	32235	1,000.00
HWSD1	R-160266-2070	BAILEY ROBERT E	4225	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2072	TYE LIVING TRUST	4221	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2074	WARREN GEORGE WAYNE TRUST ET AL	4215	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1563	2,000.00
HWSD1	R-160266-2076	WILLANDT LIVING TRUST	4211	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225-1563	2,000.00
HWSD1	R-160266-2078	MOLITORIS MICHAEL J	4205	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160266-2080	TOMLINE DARLENE	4201	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160583-0010	CARLISLE JOHN ATTICUS	11338	BEACON DR	JACKSONVILLE	FL	32225-1003	2,000.00
HWSD1	R-160583-0020	BRUINSMA AUDREY ALLISON	11308	BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160583-0030	HUDSON DONALD R	11268	BEACON DR	JACKSONVILLE	FL	32225-4044	2,000.00
HWSD1	R-160583-0040	CARROLL FRANK J	11250	BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160583-0050	BLANTON CHRISTOPHER J	11240	BEACON DR	JACKSONVILLE	FL	32225-4044	2,000.00
HWSD1	R-160583-0060	HARRELL OTIS C	11230	BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160619-0000	LOVELY WALLACE G	11350	BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160620-0000	WEST PATRICIA A TRUST	11420	STARBOARD DR	JACKSONVILLE	FL	32225-4045	2,000.00
HWSD1	R-160621-0000	JACKSON RONALD T	11430	STARBOARD DR	JACKSONVILLE	FL	32225-4045	2,000.00
HWSD1	R-160622-0000	MCMILLAN DEBRA L	11440	STARBOARD DR	JACKSONVILLE	FL	32225-4045	2,000.00
HWSD1	R-160623-0000	FOXX LATEYA	11452	STARBOARD DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160624-0000	MCFEELEY ROBERT	11462	STARBOARD DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160625-0000	BRYAN PATRICK	11474	STARBOARD DR	JACKSONVILLE	FL	32225-4045	2,000.00
HWSD1	R-160626-0000	ANDERSON JOHN	11506	STARBOARD DR	JACKSONVILLE	FL	32225-1015	2,000.00
HWSD1	R-160627-0000	HARRIS BRENDA	11518	STARBOARD DR	JACKSONVILLE	FL	32225-1015	2,000.00
HWSD1	R-160628-0000	KANE DANA	11528	STARBOARD DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160628-0010	MILL SHORT OF AN HEIR REVOCABLE TRUST	11540	STARBOARD DR	JACKSONVILLE	FL	32225-1015	2,000.00
HWSD1	R-160629-0000	PIPES STANLEY H JR	11554	STARBOARD DR	JACKSONVILLE	FL	32225-1015	2,000.00
HWSD1	R-160661-0012	HUNSAKER JANNETJE	11541	PORTSIDE DR	JACKSONVILLE	FL	32225-1518	2,000.00

**HARBOUR WATERWAY SPECIAL DISTRICT
PROPOSED 2023 NON-AD VALOREM ASSESSMENT**

CDD/SD CODE	STRAP	OWNER	PARCEL LOCATION					NON-AD VALOREM ASSESSMENT
			ADDRESS	STREET	CITY	ST	ZIP	
HWSD1	R-160661-0014	BAGLINO JOSPEH B	11529	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0016	NEWMAN RAYMOND H	11517	PORTSIDE DR	JACKSONVILLE	FL	32225-1518	2,000.00
HWSD1	R-160661-0018	WELLBORN EUGENE D LIFE ESTATE	11505	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0020	ENGLE JOANNA MYERS	11441	PORTSIDE DR	JACKSONVILLE	FL	32225-1516	2,000.00
HWSD1	R-160661-0022	METTKE J PAUL	11429	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0024	BARRANCO JOHN CHARLES JR	11415	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0026	LEVANDER THOMAS JOSEPH	11401	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0028	CHUPP HEIDI	11347	PORTSIDE DR	JACKSONVILLE	FL	32225-1516	2,000.00
HWSD1	R-160661-0030	CUGINI BRANDON JAMES	11333	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0032	BOND NEVA F ET AL	11319	PORTSIDE DR	JACKSONVILLE	FL	32225-1516	2,000.00
HWSD1	R-160661-0034	KOIVISTO JAMES H	11305	PORTSIDE DR	JACKSONVILLE	FL	32225-1516	2,000.00
HWSD1	R-160661-0036	FORD MARK	11267	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0038	TREVASKIS FAMILY TRUST	11257	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0040	HAWN JERRY J	11245	PORTSIDE DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160661-0042	MACCURREN CAROL C B/E	11231	PORTSIDE DR	JACKSONVILLE	FL	32225-1516	2,000.00
HWSD1	R-160661-0075	ANDERSON BRUCE L	11211	PORTSIDE DR	JACKSONVILLE	FL	32225-1516	2,000.00
HWSD1	R-160661-0300	MARSHALL ALAN M	4224	LEEWARD PT	JACKSONVILLE	FL	32225-1513	2,000.00
HWSD1	R-160661-0305	WHITE LANNIE D	4210	LEEWARD PT	JACKSONVILLE	FL	32225-1513	2,000.00
HWSD1	R-160661-0308	GIBSON TERRY L	4174	LEEWARD PT	JACKSONVILLE	FL	32225-1512	2,000.00
HWSD1	R-160661-0310	MINCY JORDAN	4156	LEEWARD PT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160663-0000	OAK LANDINGS RD TRUST	0	FT CAROLINE RD	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160663-1210	OAK LANDINGS RD TRUST	0	OAK LANDINGS DR	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160663-1220	160663 1220 TRUST	0	HARBOUR ISLAND DR	JACKSONVILLE	FL	32225	500.00
HWSD1	R-160671-0060	BAISDEN MARILYN M	4410	BEACON DR	JACKSONVILLE	FL	32225-1001	2,000.00
HWSD1	R-160671-0070	JOYCE HAYES TRUST	4418	W BEACON DR	JACKSONVILLE	FL	32225-1001	2,000.00
HWSD1	R-160677-0070	FREUND BRUCE A	4426	W BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160677-0080	FORNOS RICARDO LIFE ESTATE ET AL	4434	W BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160677-0090	CHUN CONRAD C	4450	W BEACON DR	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160677-0100	WINKLER GREGORY F	4458	W BEACON DR	JACKSONVILLE	FL	32225-1001	2,000.00
HWSD1	R-160684-5028	WILLIAMS STACI S	0	HARBOR CAY CT	JACKSONVILLE	FL	32225	0.00
HWSD1	R-160684-5033	SUGGS STACI S	11000	HARBOR CAY CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-5035	RIVENBURGH CHRISTINA	11002	HARBOR CAY CT	JACKSONVILLE	FL	32225-4043	2,000.00
HWSD1	R-160684-5045	KEANE CHRISTOPHER MARK	11018	HARBOR CAY CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-5050	WHALEY MAARSHALL ET AL	11034	HARBOR CAY CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7021	WALKER TRENT J	4456	BAY HARBOUR DR	JACKSONVILLE	FL	32225	2,000.00

**HARBOUR WATERWAY SPECIAL DISTRICT
PROPOSED 2023 NON-AD VALOREM ASSESSMENT**

CDD/SD CODE	STRAP	OWNER	PARCEL LOCATION					NON-AD VALOREM ASSESSMENT
			ADDRESS	STREET	CITY	ST	ZIP	
HWSD1	R-160684-7024	ST GERMAIN PETER ALBERT	4464	BAY HARBOUR DR	JACKSONVILLE	FL	32225-1046	2,000.00
HWSD1	R-160684-7027	LAVELLE CHRISTOPHER A	4472	BAY HARBOUR DR	JACKSONVILLE	FL	32225-1046	2,000.00
HWSD1	R-160684-7051	CARTER JERRY W	4455	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1084	2,000.00
HWSD1	R-160684-7054	DELUCIA THERESA W	4449	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1084	2,000.00
HWSD1	R-160684-7057	SHELFER MARGARET S	4452	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1083	2,000.00
HWSD1	R-160684-7060	CLARE JONATHAN ANDREW	4460	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7063	MCANENY LEONARD WILLIAM	4468	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1083	2,000.00
HWSD1	R-160684-7066	SHOUP RYAN	4476	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7069	HALE LARRY G	4484	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7072	POOLE STANLEY O	4492	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1083	2,000.00
HWSD1	R-160684-7075	PEPER RICHARD C JR	4510	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1079	2,000.00
HWSD1	R-160684-7078	DOHERTY JOANNE K	4518	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1079	2,000.00
HWSD1	R-160684-7104	SWANSON TRUST	4526	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1079	2,000.00
HWSD1	R-160684-7106	TIETJEN IAN SWEENEY	4534	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7108	MCDILL AUDREY A	4544	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1079	2,000.00
HWSD1	R-160684-7110	STRONSKI JAMES A	4552	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7112	SHEQI ROLAND	4560	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7114	SCOTT STEVEN C	4574	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7116	MCCLAIN CLYDE D JR	4596	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1079	2,000.00
HWSD1	R-160684-7205	CREGAR ROBERT	4620	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7210	BURT ARTHUR WADSWORTH JR ET AL	4628	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7215	D&G LAND TRUST	4636	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7220	WHITE JAMES M LIVING TRUST	4644	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1085	2,000.00
HWSD1	R-160684-7225	STEVENS DIANA L LIFE ESTATE	4650	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
HWSD1	R-160684-7230	BRANDE MICHAEL L	4658	HARBOUR NORTH CT	JACKSONVILLE	FL	32225-1085	2,000.00
HWSD1	R-160684-7235	PEFFERLE DREW CORY	4666	HARBOUR NORTH CT	JACKSONVILLE	FL	32225	2,000.00
								\$ 223,500.00

HARBOUR WATERWAY SPECIAL DISTRICT

Motion to Disburse Funds:

Tuesday, June 13, 2023

Date	Num	Description	Memo	Amount
CURRENT ASSETS				
4/30/2023		TRUIST CHECKING ACCOUNT	BEGINNING BALANCE	\$ 2,988,556.71
		TAX DEPOSITS	May 1 -31	2,992.56
TOTAL GENERAL FUND BALANCE				\$ 2,991,549.27
CLEARED DISBURSEMENTS				
5/6/2023	Trans	Truist Credit Card	Payment - Billing Cycle Date	(1,720.00)
5/26/2023	1993	Caroline Birtalan	Administrative Services (March 14)	(150.00)
5/23/2023	Epay	Lewis Longman & Walker	Legal Services up to: (April Billing)	(450.00)
5/5/2023	Debit	Stanley Pipes	District Manager 45.50 hrs. - (April Billing)	(3,678.93)
5/9/2023	Debit	USA IRS - Tax Payment	Payroll & Withholding Taxes - April	(1,330.58)
5/15/2023	Debit	Truist Bank	Truist Merchant Services - Fees	(90.85)
5/24/2023	1992	James Doherty	Landscape Service - Marina, Marsh, & Entrance (April)	(270.00)
5/11/2023	1989	JAX AA Fencing	Fencing for Marina	(1,969.57)
5/12/2023	Debit	Duval Tax Collector	Tax Certificate deposit	(1,200.00)
5/30/2023	Debit	Duval Tax Collector	Tax Certificate - Purchase of 8 tax certificates	(7,004.61)
Ongoing		2021 Tax Rebate Program	Rebate Checks	-
DISBURSEMENTS - SubTotal				(17,864.54)
5/31/2023		TRUIST CHECKING ACCOUNT	TOTAL GENERAL FUND ENDING BALANCE	\$ 2,973,684.73
OUTSTANDING DISBURSEMENTS / DEPOSITS				
6/5/2023	Debit	Stanley Pipes	District Manager up to 59.75 hrs. - (May Billing)	(5,975.00)
4/8/2023	Debit	JEA - Marina	Monthly Bill - (04/27/2023)	(40.56)
5/25/2023	Debit	JEA - Marina	Monthly Bill - (05/27/2023)	(46.14)
6/5/2023	1996	James Doherty	Landscape Service - Marina, Marsh, & Entrance (June)	(270.00)
SubTotal				(6,331.70)
TOTAL GENERAL FUND BALANCE - after Outstanding Items				\$ 2,967,353.03
REQUESTED DISBURSEMENTS				
6/5/2023	1997	Caroline Birtalan	Administrative Services (May 9 & 23)	(300.00)
6/5/2023	Debit	Stanley Pipes	District Manager up to 60.00 hrs. - (June Billing)	(6,000.00)
6/5/2023	Debit	USA IRS - Tax Payment	Payroll & Withholding Taxes - May	(1,219.14)
6/5/2023	Debit	Truist Bank	Truist Merchant Services - Fees	(90.85)
6/5/2023	Epay	Lewis Longman & Walker	Legal Services up to: (May Billing)	(925.00)
6/5/2023	Trans	Truist Credit Card	Payment - Billing Cycle Date 6-10-2023	(450.00)
6/5/2023		Decks & Dock Lumber Co.	Ramps for Marina	(5,000.00)
SubTotal				(13,984.99)
TOTAL AVAILABLE FUNDS AFTER REQUESTED DISBURSEMENTS				\$ 2,953,368.04
PLANNED PROJECT EXPENSES				
Ongoing		Parcel Owners	Purchase marsh & other parcels adjacent or near to the District	(300,000.00)
Ongoing		Equipment Rentals / Labor/ Supplies	COJ Park Development: up to	(30,000.00)
6/30/2023	1	Marina Development Project	(1) Upgrade security and replace gate, replace electrical service; (2) Replace bulkhead; (3) Extend Boat Ramp	(144,000.00)
9/15/2023	2	South Bulkhead Replacement - 1300 ft	Replace bulkhead out to power lines - live wall or bulkhead	(950,000.00)
6/15/2023	3	Powerline Dredging Project	Remove up to 30,000 cubic yards from powerlines to the first house	(450,000.00)
6/30/2023	4	Reed Island Park	HWSD acquires 77.7 acre park from COJ & manage park	(850,000.00)
12/31/2023	5	Reed Island Park	Sell (4) four river front lots	850,000.00
TOTAL PLANNED PROJECTS:				\$ (1,874,000.00)
FORECAST NET REVENUE FROM 2022 ASSESSMENT				\$ 7,354.22
2022 Assessment Collected		\$	206,646	
BUDGETED OPERATING EXPENSES - June 1, 2023 thru June 30, 2023				(31,021.71)
OPERATING EXPENSES & DEBT SERVICE EXPENSE:				\$ (31,021.71)
TOTAL HWSD PROJECTED DISPOSABLE FUNDS				
TOTAL PROJECTED AVAILABLE FUNDS after FY Operating & Project Expenses				\$ 1,055,700.55

HARBOUR WATERWAY SPECIAL DISTRICT

Motion to Disburse Funds:

Tuesday, July 11, 2023

Date	Num	Description	Memo	Amount
CURRENT ASSETS				
5/31/2023		TRUIST CHECKING ACCOUNT	BEGINNING BALANCE	\$ 2,973,684.73
		TAX DEPOSITS	June 1 - 30	5,466.73
		Truist Merchant Services		5.00
TOTAL GENERAL FUND BALANCE				\$ 2,979,156.46
CLEARED DISBURSEMENTS				
6/26/2023	Trans	Truist Credit Card	Payment - Billing Cycle Date	(194.79)
6/30/2023	Trans	Truist Credit Card	Payment - Billing Cycle Date	(209.91)
6/7/2023	1997	Caroline Birtalan	Administrative Services (March 14)	(300.00)
6/2/2023	Debit	Stanley Pipes	District Manager up to 59.75 hrs. - (May Billing)	(4,678.91)
6/6/2023	Debit	USA IRS - Tax Payment	Payroll & Withholding Taxes - May	(1,219.14)
6/15/2023	Debit	Truist Bank	Truist Merchant Services - Fees	(90.85)
6/27/2023	1996	James Doherty	Landscape Service - Marina, Marsh, & Entrance (May)	(270.00)
6/30/2023	Debit	Stanley Pipes	District Manager up to 58.75 hrs. - (June Billing)	(4,550.56)
4/8/2023	Debit	JEA - Marina	Monthly Bill - (04/27/2023)	(40.56)
5/25/2023	Debit	JEA - Marina	Monthly Bill - (05/27/2023)	(46.14)
Ongoing		2021 Tax Rebate Program	Rebate Checks	-
DISBURSEMENTS - SubTotal				(11,600.86)
6/30/2023		TRUIST CHECKING ACCOUNT	TOTAL GENERAL FUND ENDING BALANCE	\$ 2,967,555.60
OUTSTANDING DISBURSEMENTS / DEPOSITS				
7/5/2023	Debit	JEA - Marina	Monthly Bill - (06/27/2023)	(49.76)
	2000	James Doherty	Landscape Service - Marina, Marsh, & Entrance (June)	(270.00)
7/10/2023	Epay	Lewis Longman & Walker	Legal Services up to: (May Billing)	(925.00)
7/7/2023		USA IRS - Tax Payment	Form 2290 - Heavy Vehicle Tax	(550.00)
				SubTotal
				(1,794.76)
TOTAL GENERAL FUND BALANCE - after Outstanding Items				\$ 2,965,760.84
REQUESTED DISBURSEMENTS				
7/11/2023	2001	Caroline Birtalan	Administrative Services (June 13)	(150.00)
7/11/2023	Debit	Stanley Pipes	District Manager up to 65.00 hrs. - (July Billing)	(6,500.00)
7/11/2023	Debit	USA IRS - Tax Payment	Payroll & Withholding Taxes - June	(3,527.06)
7/11/2023	Debit	Truist Bank	Truist Merchant Services - Fees	(90.85)
7/11/2023	Epay	Lewis Longman & Walker	Legal Services up to: (June Billing)	(1,500.00)
7/11/2023	Trans	Truist Credit Card	Payment - Billing Cycle Date 7-10-2023	(285.59)
7/31/2023		Decks & Dock Lumber Co.	Ramps for Marina	(5,000.00)
8/1/2023		James Doherty	Landscape Service - Marina, Marsh, & Entrance (July)	(270.00)
				SubTotal
				(17,323.50)
TOTAL AVAILABLE FUNDS AFTER REQUESTED DISBURSEMENTS				\$ 2,948,437.34
PLANNED PROJECT EXPENSES				
Ongoing		Parcel Owners	Purchase marsh & other parcels adjacent or near to the District	(300,000.00)
Ongoing		Equipment Rentals / Labor/ Supplies	COJ Park Development: up to	(30,000.00)
6/30/2023	1	Marina Development Project	(1) Upgrade security and replace gate, replace electrical service; (2) Replace bulkhead; (3) Extend Boat Ramp	(239,000.00)
9/15/2023	2	South Bulkhead Replacement - 1300 ft	Replace bulkhead out to power lines - live wall or bulkhead	(910,000.00)
6/15/2023	3	Powerline Dredging Project	Remove up to 30,000 cubic yards from powerlines to the first house	(450,000.00)
6/30/2023	4	Reed Island Park	HWSD acquires 77.7 acre park from COJ & manage park	(850,000.00)
12/31/2023	5	Reed Island Park	Sell (4) four river front lots	850,000.00
TOTAL PLANNED PROJECTS:				\$ (1,929,000.00)
FORECAST NET REVENUE FROM 2023 ASSESSMENT				\$ 205,500.00
2023 Assessment Collected				\$ -
BUDGETED OPERATING EXPENSES - August 1, 2023 thru June 30, 2024				(128,659.93)
OPERATING EXPENSES & DEBT SERVICE EXPENSE:				\$ (128,659.93)
TOTAL HWSD PROJECTED DISPOSABLE FUNDS				
TOTAL PROJECTED AVAILABLE FUNDS after FY Operating & Project Expenses				\$ 1,096,277.41

HARBOUR WATERWAY SPECIAL DISTRICT

CREDIT CARD TRANSACTIONS - STANLEY PIPES

Tuesday, June 13, 2023

Date	Description	Memo	Government	Reed Island	Total Amount	Outstanding Balance
POSTED TRANSACTIONS						
4/10/2023	STATEMENT CYCLE DATE	CREDIT CARD STMT BALANCE			\$ (63.97)	\$ (63.97)
4/28/2023	Truist Checking Account	Credit Card Payment	63.97		63.97	-
4/29/2023	Intuit QuickBooks	Quickbooks Software Renewal - Enterprise	(1,720.00)		(1,720.00)	(1,720.00)
5/6/2023	Truist Checking Account	Credit Card Payment	1,720.00		1,720.00	-
5/10/2023	STATEMENT CYCLE DATE	CREDIT CARD STMT BALANCE			\$ -	\$ -
5/17/2023	Financial News & Daily Record	Public Notice - Special Meeting	(30.00)		(30.00)	(30.00)
6/8/2023	Financial News & Daily Record	Public Notices - Meeting Schedule	(59.38)		(59.38)	(89.38)
6/8/2023	Financial News & Daily Record	Public Notices - Public Hearing non-Ad Valorem	(59.38)		(59.38)	(148.76)
6/6/2023	City of Jacksonville	Parking	(5.00)		(5.00)	(153.76)
6/6/2023	City of Jacksonville	Parking	(5.00)		(5.00)	(158.76)
6/7/2023	City of Jacksonville	Parking	(7.03)		(7.03)	(165.79)
6/10/2023	STATEMENT CYCLE DATE	CREDIT CARD STMT BALANCE			\$ (165.79)	\$ (165.79)
6/14/2023	City of Jacksonville	Parking	(10.00)		(10.00)	(175.79)
6/21/2023	City of Jacksonville	Parking	(10.00)		(10.00)	(185.79)
6/22/2023	City of Jacksonville	Parking	(9.00)		(9.00)	(194.79)
6/27/2023	Truist Checking Account	Credit Card Payment	194.79		194.79	-
6/28/2023	City of Jacksonville	Parking	(10.00)		(10.00)	(10.00)
6/29/2023	Sam's Club	HP 952XL ink cartridges	(199.91)		(199.91)	(209.91)
7/2/2023	Truist Checking Account	Credit Card Payment	209.91		209.91	-
7/6/2023	www.1 and 1.com	Website Hosting	74.97		74.97	74.97
7/7/2023	Express Truck Tax	2290 Heavy Truck Tax		21.39	21.39	96.36
7/8/2023	Gate	Diesel Fuel		175.00	175.00	271.36
7/8/2023	Gate	Diesel Fuel		14.23	14.23	285.59
7/11/2023		OUTSTANDING BALANCE				\$ 285.59