

**THIRD PARTY NETWORK ACCESS AND  
CONFIDENTIALITY AGREEMENT WITH  
THE SAN DIEGO UNIFIED PORT DISTRICT**

1. AGREEMENT INTRODUCTION

1.1. Objective

To protect the San Diego Unified Port District Information Assets against a variety of threats including: loss, destruction, modification, duplication, inappropriate disclosure, unauthorized access, diversion (redirection), misuse, or theft.

1.2. Background

This Third Party Network Access and Confidentiality Agreement address' the need for information security and applies to all Contractors, Consultants, and third party users of Information or Information Systems belonging to the San Diego Unified Port District (District).

The District relies upon the regular flow of information and Information Systems to manage and record information. Although not officially recognized in the financial records of most organizations, information is therefore, a valuable and critical asset. Information is also an essential resource that is used as an input to every product and service that the District provides. Without accurate, timely, and adequately protected information, the District would not be able to serve as the trusted steward to the San Diego tidelands that it was legislated to be.

In addition, the District, because of its special governmental status, is held accountable to various pieces of State Legislation that dictate the availability of information to its trustees. As a result, Information Systems security has become a critical factor in the protection of the District's information assets. In recognition of this fact, the Information Technology Department now acts as a guardian for all Information Systems security and related issues.

Effective information security requires a team effort, involving the participation and support of everyone using the District's Information Systems. In recognition of the need for teamwork, this Agreement established the roles and responsibilities of Custodians who have access to District Related Data or Information Systems as well as the expectations a person has as a Custodian to help protect District Related Data and Information Systems from a variety of threats including: loss, destruction, modification, duplication, inappropriate disclosure, unauthorized access, diversion (redirection), misuse, or theft.

1.3. California Public Records Act

1.3.1. Confidential Classification

Under the California Public Records Act the "Confidential" classification applies to sensitive business information that is specifically exempt from disclosure under the terms of the Act. Confidential information is intended strictly for use within the District and a limited number of pre-determined trusted third parties. Its unauthorized disclosure could adversely impact the District, its business partners, and/or its customers. Although not representative of an exhaustive list, examples include information relating to contracts under negotiation, acquisition plans, and documents concerning existing litigation, police records, employee performance evaluations, Homeland Security records, and certain information belonging to third parties that has been entrusted to the District.

1.3.2. Public Classification

Under the California Public Records Act, the classification "Public" applies to all information held within the District that is not specifically exempted as "Confidential." By definition, however, there is no such thing as unauthorized disclosure of public information. It is, therefore, often difficult to determine whether information is "public" or in fact "confidential". For this reason The District has established a procedure by which any member of the public can obtain information. This procedure is called the Public Records Request.

Initials: \_\_\_\_

However, information obtained through Custodial access has not been vetted through the Public Record Request procedure. The District has therefore adopted a standing classification for information that is obtained through custodianship rather than through the California Public Records Act. All Information obtained by a Custodian by accessing the District Information Systems will be considered **confidential**.

2. DEFINITIONS

*Business need for Information* - For each Custodian this need is determined in the Agreement as the Scope of Work. The Custodian's need to know extends only to the extent of accomplishing the assignment determined in the Agreement's Scope of Work.

*Computer Virus*: - An unauthorized program that replicates itself, attaches itself to other programs, and spreads onto various data storage media (floppy disks, magnetic tapes, random access memory, etc.) and/or across a network. The symptoms of virus infection include much slower computer response time, erratic Systems behavior, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers.

*Custodian*: - Persons in physical or logical possession of either District Related Data or Information Systems. There are two kinds of custodians. The first kind are those that have been assigned workstations at District facilities and/or District owned computer for the purpose of accomplishing an assignment that is predetermined by a contractual agreement. The second kind of custodians are those that work from a remote location, using their own equipment to gain access through Citrix to a District server for the purpose of accomplishing an assignment that is predetermined by a contractual agreement. Since either methods of access pose the same risk to the District, the measures put into place by this procedure are the same for each unless otherwise called out.

The best way to decide if a person is a Custodian of District Related Data or Information Systems is to establish if a that person has signed their own Third Party Network Access and Confidentiality Agreement. Simply being knowledgeable of the concepts of this agreement does not determine a Custodial right to District Related Data or Information Systems.

*District Related Data*: - Used to refer to all manifestations of data both electronic and paper including, microfilm, Diskettes, CD's DVD's, flash drives and Tapes.

*Information Systems*: - A System, belonging to the District, that is comprised of any and all desktop computers, servers, and infrastructure to include cabling, routing, switching, firewall and any peripheral in relation.

*Service Provider Agreement*: - A legally binding document that the Custodian's sponsoring company has negotiated and executed with the Board of Port Commissioners or its designee for services defined in a Scope of Work. The Custodian's access to District Related Data or Information Systems is limited to the specifications found in the Service Provider's Agreement's Scope of Work. A Custodian may not enter into the Third Party Network Access Procedure and Confidentiality Agreement without first being assigned to provide services to the District by the negotiation of such a Service Agreement.

*Sponsor*: - Department Managers or their delegates within the District who bear responsibility to the Executive Director for the letting of contracts that employ Vendors, Consultants, or Temporary services.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
Sponsor	Ensures Custodians are using District Related Data and Information Systems in a way that is commensurate with this Agreement. All District Related Data or Information Systems must have a designated Sponsor. For each type of District Related Data or Information Systems, the Sponsors define its need to know and who will be permitted to access it, and define its authorized uses.
Custodian	Custodians are responsible for safeguarding District Related Data, and Information Systems including implementing access control systems to prevent inappropriate disclosure, and making back-ups of

Initials: \_\_\_\_

	District Related Data stored on a computer so that critical information will not be lost. When District Related Data is in any other form, Custodians are required to keep it out of sight and reach of those individuals who are not deemed the Custodian of the District Related Data. Custodians are also required to adhere to all statements and provisions of the Third Party Network Access and Confidentiality Agreement
District's IT Department	Acts as Guardian to all District Related Data and Information Systems. Retains the right to remove anyone from its Information Systems that does not comply with all regulations called out in the Third Party Network Access and Confidentiality Agreement. Monitors Information System activity and Maintains the concepts administered under this Agreement.

4. HANDELING OF DISTRICT RELATED DATA

4.1. Authorized Uses of District Related Data

District Related Data or Information Systems is permitted to be used only for the purposes expressly authorized by the Sponsor in the Agreement's Scope of Work. Being granted access of District Related Data or Information Systems does not give the Custodian the right to make further determinations of its availability to additional parties. Should the Custodian feel that it is necessary to share District Related Data or Information Systems in the effort to achieve the level of service determined in the Agreement's Scope of Work, they are required to receive prior written consent from the Sponsor of that information.

4.2. Consistent Protection of District Related Data or Information Systems

While in the possession of the Custodian, it is the Custodians duty to consistently protect District Related Data and Information Systems. This means from its origination until the time it is returned to the District no matter where it resides, no matter what form it takes, no matter what technology was used to handle it, and no matter what purpose(s) it serves. In order to achieve consistent protection, custodians will be expected to apply and extend the concepts of the Third Party Network Access and Confidentiality Agreement to fit the needs of day-to-day operations.

4.3. Inadvertent Disclosure of District Related Data

Custodians handling District Related Data must be vigilant to make sure that it is not inadvertently disclosed to people who have not been designated as Custodians. Custodians must not leave media containing District Related Data on their desks or in unlocked cabinets unless the District Related Data is protected through encryption. In addition, Custodians must not leave their desktop computers, workstations, or terminals unattended without first logging-out or invoking a screensaver with password protection.

4.4. Storage of District Related Data

Custodians must not use their local machines for the storage of important District Related Data. This data is not backed up and could be unrecoverable should a hardware, software, or human error occur. In addition, District Related Data stored locally is not protected from being read or copied by persons unauthorized to do so. Custodians using District equipment to perform the Agreement's Scope of Work must store all District Related Data on the District's central file servers. These servers are backed up on a frequent basis and have fault tolerant capabilities that guard against data loss. Local machines may be used for drafting correspondence, performing analysis of District Related Data and general work in process, providing that the loss of such work would not have serious impact to the District.

4.5. Snooping

Custodians are not permitted to "snoop" through District Related Data or Information Systems. For example, where a Custodian discovers that they can access directories (e.g. the personal directories of others), which they suspect are not necessary to accomplish the Agreement's Scope of Work, they are to

exit the directory immediately and report its availability to the Sponsor. Curious searching for interesting files and/or programs is absolutely prohibited.

#### 4.6. Message Privacy is not Guaranteed

Because the District is a special governmental agency and subject the California Public Records Act, Custodians must expect that NO communication or record be private. Furthermore, Custodians must be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Such communications or records may also be available to the public through Public Record Requests. Meaning that anyone, including the Media and law enforcement may at any time, and without cause, become in possession of any communications or record generated by or residing on District Information Systems.

#### 4.7. Reproduction of District Related Data

Reproduction of District Related Data, including printing additional copies via a computer printer, must only be carried out based on a valid need to support the services defined by the Agreement's Scope of Work. Likewise, extracts, summaries, translations, or derivatives of District Related Data must not be made unless they are required to support the assignments defined by the Agreement's Scope of Work. If a reproduction is made, it is subject to the same Confidentiality Requirements as the original District Related Data that was used to obtain the copy.

#### 4.8. Transportation of District Related Data

Physical transport of District Related Data requires the use of a trusted courier such as District mail staff, the US Postal Service, UPS, or Federal Express or other reputable courier service. All District Related Data sent via such couriers must be enclosed in an opaque and sealed envelope. Likewise, whenever this information is sent over computer networks not belonging to the District, such as the Internet, it must be in encrypted form. Custodians are reminded that the electronic communications passing through District Information Systems are not encrypted by default.

#### 4.9. Destruction of District Related Data or Information Systems

When the term of the Agreement has been met, any and all District Related Data or Information Systems must be returned to the Sponsor, including any and all reproductions that were made. It is not at the Custodian's discretion to destroy District Related Data. Only the District Sponsor is at liberty to determine the Data's need for destruction.

### 5. PASSWORD PROTECTION

#### 5.1. Difficult-to-Guess Passwords

Passwords are an essential component of the security of District Information Systems. To ensure that these Systems do the job they were intended to do, Custodians must choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address are not to be used. This also means passwords are not to be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang are not to be used. This is because electronic dictionaries are routinely used to "crack" a password and obtain access to a System.

Custodians must also not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, Custodians must NOT employ passwords like "X34JAN" in January, "X34FEB" in February, etc. Additionally, Custodians must not construct passwords that are identical or substantially similar to passwords they have previously employed.

#### 5.2. Password Storage

Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control Systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down and left in a place where unauthorized persons might discover them. Aside from initial password assignment and

Initials: \_\_\_\_\_

password-reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized Custodian, the password must be immediately changed. Please contact the District IT Help Desk at x7200 to facilitate.

### 5.3. Password Constraints

To make guessing more difficult, passwords must also be at least six characters long wherein two password characters are required to be something other than alpha characters. To ensure that a compromised password is not misused on a long-term basis, passwords will be changed every 60 days.

### 5.4. Sharing Usernames and Passwords

Regardless of the circumstances, usernames or passwords must never be shared or revealed to anyone. To do so exposes the authorized custodian to responsibility for actions that the unauthorized party may make with the disclosed username or password. If Custodian needs to share computer-resident District Related Data with other custodians in order to accomplish the assignment in the Agreement's Scope of work, they must use electronic mail or public directories on the District's local area network servers to accomplish this.

## 6. SYSTEM USE AND PRIVILEGES

### 6.1. Internet Activity Monitoring

Custodians must be aware that all World Wide Web activity performed on District Information Systems will be monitored electronically. This monitoring may be used to measure the Custodian's performance as it is related to this Agreement, as well as to protect the District's information assets.

### 6.2. Appropriate Sites

Custodians using District computers who discover they have unintentionally connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material must immediately disconnect from that site. While the District will attempt to block access from inappropriate sites, the ability to connect with a specific web site does not in itself imply that Custodians are permitted to visit that site. The District reserves the right to monitor and log all web sites visited.

### 6.3. Message Interception

Wiretapping and other types of message interception are straightforward and frequently encountered on the Internet. Accordingly, District Related Data must not be sent over the Internet unless it has first been encrypted by approved methods. The SSL (secure socket layer) or SET (secure electronic transaction) encryption processes are both acceptable Internet encryption standards for the protection of District Related Data. Other encryption processes, such as PGP ("pretty good privacy"), are permissible with the approval of the District's IT Department. If there is ever a doubt, consult the District's IT Department or the Agreement Sponsor prior to sending the information.

### 6.4. Public Representations

Custodians, while using District Information Systems, directly or indirectly indicate their affiliation with the District in mailing lists (listservs) or other offerings on the Internet. This is done by explicitly adding certain words, or it may be implied, for instance via an electronic mail address. Regardless, whenever Custodians participate in such offering on the Internet, they must also clearly indicate the opinions expressed are their own, and not necessarily those of the District. Likewise, while using District Information Systems, any political advocacy statements and/or product/service endorsements are prohibited. With the exception of ordinary marketing and customer service activities, the Sponsor must clear all such representations on behalf of the District in writing.

## 7. SYSTEM VIRUSES

### 7.1. Prevention of Viruses

Initials: \_\_\_\_\_

Custodians connecting to District Information Systems with equipment not provided by the District are required to be current with operating systems security patches and protected by industry standard viral protection software.

District Equipment that is issued to a Custodian to perform the assignment defined in the Scope of Work is already protected with viral protection software. Any System security patches required for equipment issued by the District will be done by the District's Information Technology Department.

## 7.2. Virus Eradication

If Custodian suspects a computer virus has infected their equipment, they must immediately stop using the involved computer. If Custodian is using District issued Equipment, Please contact the District IT Help Desk at x7200 to facilitate. Disks and other storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. Custodians using District issued equipment are not permitted to attempt to eradicate viruses themselves; The District's IT Department staff will be called in to complete this complex task in a manner that is consistent with District Procedures.

## 8. SOFTWARE

### 8.1. Approved Software

If the District has issued a workstation to a Custodian, the Custodian is not permitted to run additional software programs other than what was supplied with the workstation. If the Custodian finds that additional software packages are needed to accomplish the goals of the Agreement's Scope of Work, they must consult their Sponsor. Custodian is not permitted to do any of the following with District Software or District Information Systems:

- **Install Software** - District Information Systems are organization-owned assets and must be kept both software-legal and virus-free. If working on a District issued workstation, Custodian must not bring software from home nor install any non-District-owned software or load it onto any District computer.
- **Download Software** - Downloading software from the Internet or any other online source to District issued equipment is strictly prohibited. Custodians are also not permitted to run automatic software installation routines on District Information Systems.
- **Software Sharing** - Likewise, Custodians may not give software to any outsider parties including clients, contractors, customers, and others.
- **Software Duplication** - It is the procedure of the District to respect all computer software copyrights and to adhere to the terms of all software licenses to which the District is a party. Custodians may not duplicate any software licensed by the District for use either on District premises or elsewhere. Unauthorized duplication of software may subject custodians and/or the District to both civil and criminal penalties under the United States Copyright Act.
- **Push Technology** - Automatic updating of software or information on District provided computers via background "push" Internet technology (e.g. Pointcast) is not permitted. While powerful and useful, this new technology could be used to spread viruses, and cause other operational problems such as System unavailability. Often times Push technology is used to automatically install or update software across the Internet. Note that this is not the same as downloading a file to the local System and then installing it.
- **Shareware or Freeware** - Shareware is copyrighted software that is distributed freely through bulletin boards, the Internet and online services. Most freeware license agreements strictly prohibit use in a corporate environment; furthermore, it is the procedure of the District to pay software authors the fee they specify for use of their product. Acquisition and registration of shareware/freeware products will be handled in the same way as for commercial products and will be held to the same System Use and Privileges expectations as all other software outlined in the Agreement.

### 8.2. Quarterly Audits

Initials: \_\_\_\_\_

The District's IT Department will regularly conduct random or surprise software audits on all District Information Systems to ensure that the District is in compliance with all software licenses. Full cooperation of the Custodian is required during these audits. If, during one of these audits, the Custodian is found to have unauthorized software packages resident on their District issued workstation, the software may be removed from District issued equipment without prior notice to the Custodian.

### 8.3. Penalties and Reprimands

According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages as much as \$100,000 per title infringement and criminal penalties, including fines as much as \$250,000 per title infringed and imprisonment of up to five years. Any Custodian who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the particular circumstance. Such discipline may include termination of the Service Provider Agreement and or suspension of Custodial System privileges. The District does not condone the illegal duplication or use of software and will not tolerate it.

## 9. TAMPERING WITH DISTRICT INFORMATION SYSTEMS

### 9.1. Systems Security

Unless through an agreed upon Scope of Work, Custodians are not permitted to test, or attempt to compromise District Information System security measures. Incidents involving unapproved System cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures are unlawful, and will be considered serious violations of the Third Party Network Access and Confidentiality Agreement. Likewise, short-cuts bypassing Systems security measures, as well as pranks and practical jokes involving the compromise of District Information Systems security measures are absolutely prohibited.

Computer equipment supplied by the District must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) except by the District of San Diego's IT Department. Nor shall Custodian change operating System configurations, upgrade existing operating Systems, or install new operating Systems. If such changes are required, they will be performed by the District's IT Department (in person or remotely)

### 9.2. Security Compromise Tools

Unless specifically authorized by the IT Department, Custodians are not permitted to acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise District Information Systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

### 9.3. Physical Relocation

Unless otherwise specified in writing by the Sponsor, Information Systems or any portion thereof, may NOT be moved from its given location or taken outside of District property by a Custodian. Furthermore, Custodian's are not permitted to move paper documents, files, CD's, diskettes from the location given unless written authorization is obtain by the Sponsor. If so, Custodian must use a trusted courier such as District Mail Staff, US Postal Service, UPS, Federal Express or other trusted courier. In the event District Related Data needs to be relocated using one of these couriers, the District Related Data must be sealed in an opaque envelope.

## 10. APPROPRIATE USES OF DISTRICT INFORMATION SYSTEMS

### 10.1. Personal Use

The District's code of conduct prohibits Custodians from using District time, facilities, equipment or supplies for private gain or advantage. Non-business uses of the District's computers, such as for games or extended Internet browsing (referred to as "surfing the web"), are not permitted. Custodians must not employ the Internet or other District Information Systems in such a way that the productivity of others is eroded; examples include chain letters and solicitations. Custodians must not allow unauthorized persons such as visitors or children to alter or otherwise use District Information Systems.

### 10.2. Harassing or Offensive Materials

Initials: \_\_\_\_\_

The District's Information Systems are not intended to be used for, and must not be used for the exercise of the custodians' right to free speech including but not limited to e-mail or postings to newsgroups. To avoid libel, defamation of character, and other legal problems, Custodians are not permitted to write attacks in a message or posting (referred to as "flaming"). Nor are they permitted to send messages intended to harass, annoy, alarm, or make threats against another individual or organization.

### 10.3. Contents of Messages

Custodians are not, under any circumstances, permitted to use profanity, obscenities, or derogatory remarks in electronic mail messages. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. Special caution is warranted because back-up and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

### 10.4. Unbecoming Conduct

Conduct that interferes with the normal and proper operation of the District's Information Systems, which adversely affects the ability of others to use these Information Systems, or which is harmful or offensive to others will not be permitted. Custodians must remember that any information generated or passed through the District's computer and communications System become public record and is therefore liable to be called upon and surrendered to any requesting party, for any reason. The conduct of Custodian in this respect must reflect the utmost decorum at all times.

### 10.5. Establishing Access Paths

Custodians, while using District Information Systems, are not permitted to establish electronic bulletin boards, local area networks, or modem connections to existing computer Systems, local area networks, or other multi-user Systems for communicating information. Likewise, new types of real-time connections between two or more in-house computer Systems are not permitted to be established. This Agreement helps to ensure that all District Information Systems have the controls needed to protect other connected Systems. The actual security of a network-connected computer is not just a function of that machine's security mechanisms; it is also a function of all other connected Systems.

### 10.6. Access Control

Custodians, either using District issued equipment or bringing their own equipment on site to connect to the Internet are not permitted to use dial-up lines and individual modems to access the Internet. Instead, all Internet activity must pass through District firewalls so that access controls and related security mechanisms can be applied.

### 10.7. Establishing Network Connections

Custodians using District equipment are not permitted to establish Internet or other external network connections that could allow others to gain access to District Information Systems. This includes permanent connections to Internet web pages and ftp servers.

### 10.8. Spoofing

Unless tools like digital signatures and digital certificates are employed, it is relatively easy to spoof or masquerade as the identity of another on the Internet. A Custodian is not permitted to release any internal District information without first confirming the identity of the individuals and organizations contacted. Identity confirmation is ideally performed via digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third party references, and telephone conversations may be used.

### 10.9. Custodial Identity

Custodians must not attempt to misrepresent, obscure, suppress, or replacing their identity on the Internet or any District electronic communications System. The username, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. If custodians have a need to employ re-mailers or other anonymous facilities, they must do so on their own time, with their own information Systems, and with their own Internet access accounts. Use of anonymous FTP log-ins, anonymous UUCP log-ins, HTTP (web) browsing, and other access methods established with the expectation that Custodians would be anonymous are permissible.

## 11. INFORMATION RELIABILITY

### 11.1. E-mail Reliability

E-mail is not considered to be a reliable method of communication and should not be relied upon for communicating on matters of importance. If e-mail is utilized for business communications, its receipt by the intended recipient should be verified either via a telephone call or by the recipient's response to the message indicating that it was received. The "return receipt" functionality in e-mail should not be utilized for this purpose as it has the same vulnerabilities as the original e-mail message.

### 11.2. Information Reliability

If Custodian is using District issued equipment, all information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet. A considerable amount of this information is outdated and inaccurate, and in some instances is even deliberately misleading.

## 12. INSPECTION AND MONITORING

### 12.1. Regular Message Monitoring

It is not a District procedure to regularly monitor the content of electronic communications that are received or delivered using District Information Systems, however the District reserves the right to, at any time and upon its own discretion, carryout such monitoring to support operational procedures that include but are not limited to audit measures, security measures, and investigative activities.

### 12.2. Right of Examination

All information stored on or transmitted by District Information Systems is considered to be District Related Data and therefore, District property. To properly protect and manage this property, the Information Technology Department reserves the right to examine all information stored in or transmitted by these Systems. Custodians must have no expectation of privacy associated with the information they store in or send through these Systems.

## 13. AGREEMENT VIOLATIONS

### 13.1. Non-Compliance

Any Custodian who willingly, deliberately or negligently violates this Agreement will be subject to disciplinary action up to and including termination of System privileges, termination of any contractual agreement whereby Custodian is authorized to work and/or legal action as defined in the Service Provider's Agreement.

### 13.2. Mandatory Reporting

All suspected Agreement violations, System intrusions, virus infestations, and other conditions that might jeopardize District information or District information Systems must be immediately reported to the Director of Information Technology (phone 619-686-7280).

AGREEMENT STATEMENTS

I \_\_\_\_\_ (Please Print) do hereby agree by signing below that I have read and fully understand the provisions stated herein and that I will fully comply with all conditions. Furthermore, I understand that being given a Network Account and Password that I am in custody of information that is considered to be an asset of the Port of the San Diego and as such, I understand the responsibility I have as a conservator of this asset to maintain its integrity.

\_\_\_\_\_  
Custodian's Printed Name

\_\_\_\_\_  
Custodian's Signature

\_\_\_\_\_  
Date

I \_\_\_\_\_ (printed name) \_\_\_\_\_ (printed title)  
of \_\_\_\_\_ (printed company name) do hereby agree by signing below that I have authorized the above employee of my company to gain custodial access, should the District elect, of District Related Information in effort to complete the Scope of Work detailed in the Agreement on file with the District's Clerk Office as Document Number \_\_\_\_\_. I have fully read and understand the provisions stated herein as they relate to custodial access of District Related Data and that I will dutifully report any abuse of such access to the District's Information Technology Director at (619) 686-7280

\_\_\_\_\_  
Contract Executor Printed Name

\_\_\_\_\_  
Contract Executor Signature

\_\_\_\_\_  
Date



**Appendix A**  
**SAN DIEGO UNIFIED PORT DISTRICT**  
 Department of Information Technology  
 Third Party Network Account Request Form 124-003

<input type="checkbox"/> New Account <input type="checkbox"/> Change of Access <input type="checkbox"/> Expire Account		
First Name:		Last Name:
Company Name:		Supervisor:
Agreement Document number:	Start Date:	Termination Date (if applicable):
Requesting Custodian Supervisor Phone Number/email		Requesting Custodian Phone Number/email address
<b>GroupWise Distribution Lists Requested:</b> <input type="checkbox"/> <i>Everyone-District (Default)</i> <input type="checkbox"/> <i>Everyone-Airport</i> <input type="checkbox"/> <i>Everyone-Admin Bldg</i> <input type="checkbox"/> <i>Everyone-Marine</i> <input type="checkbox"/> <i>Everyone-HPHQ</i> <input type="checkbox"/> <i>Everyone-GenServ</i> <input type="checkbox"/> <i>Everyone-HPSI</i> <input type="checkbox"/> <i>Other (list below)</i>		<b>Group Memberships Requested:</b> <b>Disposition of Home Directory Files (Departing Staff):</b> Delete/Move Home Directory Files To _____ Reassign Ownership To _____
Docs Open: <input type="checkbox"/> Yes <input type="checkbox"/> NO Harbor Police: <input type="checkbox"/> RMS <input type="checkbox"/> CAD <input type="checkbox"/> PCM <input type="checkbox"/> SDOR		Synergen Role: _____ Synergen Craft: _____ SAP Access: <input type="checkbox"/> None <input type="checkbox"/> Yes (Hyperlink attached)
I, _____ agree by signing below, that I have read and fully understand the District's Third Party Network Access and Statement of Confidentiality Procedure. I fully understand that by being given a Network Account and Password that I am custodian of information that is considered to be an asset of the District. As a result, I fully understand the expectation I have as a conservator and Custodian of this Asset to maintain its integrity by adhering to all provisions outlined in this Procedure.		
<b>Custodian Signature:</b>		<b>Date:</b>
<b>Custodian Supervisor Signature:</b>		<b>Date:</b>
I, _____, The department Director of _____, agree that the above custodian requires the network access described above in order to accomplish the Scope of Work described in the Agreement stated above. I bear witness that the Custodian has been given a Sponsor as required in the Third Party Network Access and Statement of Confidentiality Procedure and that the Sponsor is aware of the limitations imposed on Custodial access to information. To that end, I take full responsibility for ensuring the Custodian and Sponsor meet the provisions of this procedure.		
<b>District Department Director's Signature:</b>		<b>Date:</b>
<b>TO BE FILLED OUT BY IT STAFF/HELP DESK PERSONNEL</b>		
Created by:		Date of Account Creation:
Custodian Login Name (Max 8 characters):		Custodian Password (To be distributed by support personnel):