

#### 1.3 OTHER RELEVANT POLICIES

The following is a list of other Board policies pertaining to information security that are managed and maintained by OTS.

- 1.3.1 Member Acceptable Usage Policy, Board Report #04-0428-PO2, as may be amended from time to time.
- 1.3.2 Student Acceptable Usage Policy, Board Report #03-0326-PO03, as may be amended from time to time.

#### 1.4 DEFINITIONS OF TERMS

#### 1.4.1 USER

Users, as defined in this policy, include all Board employees, students, contractors, consultants, temporaries, and other computer users at CPS, including those users affiliated with third parties who use Board equipment and/or access CPS data or systems.

#### 1.4.2 SERVER

A Server is defined as any computing system that is owned and/or administered by CPS which provides services to users. Examples include, but are not limited to: email systems, web servers, video conferencing devices, and file/print servers.

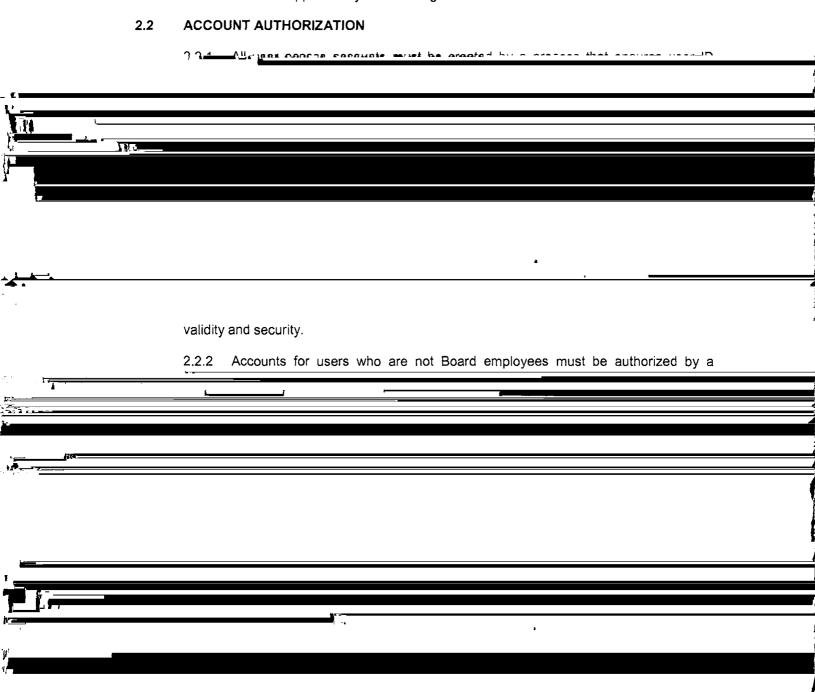
#### 1.4.3 SYSTEM ADMINISTRATOR

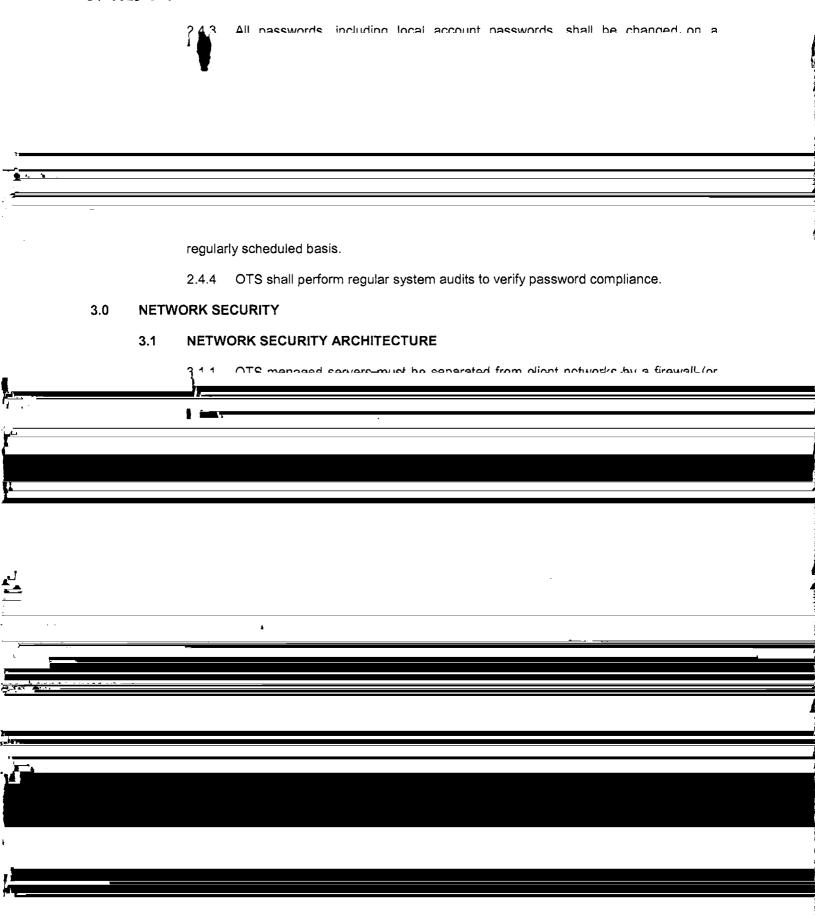
A System Administrator is defined as any Board employee, contractor, consultant,

### 2.0 USER ACCOUNTS AND ACCESS PRIVILEGES

#### 2.1 DIRECTORY SERVICES

- 2.1.1 All access-level user accounts and access credentials (for use by general users of a system or application) shall be created and maintained via enterprise directory services maintained by OTS.
- 2.1.2 Creation of separate pools of user accounts for local servers, applications, or services must be approved by OTS management.





1-	4 1.3. All servers must have all security natches and fixes applied in a timely manner
1	
<b>▲</b>	
•	
<u> </u>	
	4.1.4 All servers must have OTS standard software installed, including, but not limited
	to, remote management and anti-virus software.
	4.4. E. Alleganiers much base OTO meanagement accounts installed with administrative
· •	
) e	
<u> </u>	
-	
+X	
	rights to the machine.
	rights to the machine.
	4.1.6 All devices must have local authentication preventing unrestricted access. Local accounts and/or console access must be password protected. Local access accounts
	must adhere to security policy regarding user account, including password complexity
	requirements.
	4.1.7 All OTS managed servers must be located in approved data centers or approved
	4.1.7 All OTS managed servers must be located in approved data centers or approved

	F.O. 4. All seculations recent process unrestricted access this is asimportic implemented	
*	(- 1). 5	
		2
,		
<u> </u>		
<u></u>		
167		
		A
	· · · · · · · · · · · · · · · · · · ·	
	via a login process combined with a password protected screen saver set to engage in a	
	reasonable amount of time.	
	5.0.5 All local accounts must be password protected with passwords that adhere to	
	y*************************************	
1		
,		
	·	
	16	
	<del></del>	
<u>, , , , , , , , , , , , , , , , , , , </u>		_
, .		
en de Salanda de Lamba de la Maria de Carlos d		
<u>-न</u> ि		

# 7.0 DATA SECURITY AND APPLICATION SECURITY

	7.1	DATA CLASSIFICATION		
1				
<u>.</u> -	,			
		to sensitivity levels established by OTS.		
	7.2	DATA SECURITY		
		7.2.1 Applications that store confidential and restricted data must reside on equipment in a data-tier that is separated by a firewall (or equivalent traffic filtering). Equipment		
1				
		housing this data shall not be directly accessible by end users.		
		7.2.2 It is understood and accepted that sensitive data will always exist in a transient fashion across the network on access-tier equipment such as application servers, web		
1				
ļ				
1				

### 7.4 DATA USAGE

<u>ماغ</u>ی کام درد دا<u>است سادست مسیم میزیرا ۸</u>

use of Board data.

### 7.4.1 PERTINENT USE OF DATA

Board information shall be only used to conduct Board business. Using internal data for personal use or for professional use unrelated to Board business is forbidden.

## 7.4.2 PRIVACY AND CONFIDENTIALITY OF DATA

All users shall ensure the confidentiality of data they work with. Users are expected to respect control measures used to protect confidential and restricted data and not to

; <b>-</b>	9.1.3 CONTRACTORS, CONSULTANTS, AND OTHER BUSINESS PARTNERS			
Irl			`	
} }				
		i.		
	have their system access privileges suspended and m	ay further be subject to contract		
`E	tarmination or any athor ramedy as action deemed anne	ariata hutha Danud		
1, ===				
1 <u>14</u> 7				
			(	
•				
•	9.2 RESPONSIBILITY AND ACCOUNTABILITY			

### USERS

All individuals described in the scope section of this document are responsible and accountable for complying with the data security tenets detailed in this policy and are liable for their violation. This includes responsibility and accountability for user accounts and access to information entrusted to them by the Board and for insuring the privacy of