INFORMATION TECHNOLOGIES DIVISION

Jacksonville
Where Florida Begins.

External User Technology Use Agreement

The following policies apply to all external users of City interactive technology services

1. There is no expectation of privacy in any electronic communications, use of City property, or Internet access. City reserves the right to review, audit, or monitor any information technology used by external users.
2. Only accounts authorized by a valid representative of the Information Technologies Division (ITD) shall be used to log onto the interactive technology services.
3. External users may access only those resources for which they are specifically authorized.
4. Each person responsible for safeguarding their individual account and log on information. Passwords shall adhere to the following.
   a. Passwords shall remain confidential.
   b. Passwords shall be at least seven characters long.
   c. Passwords shall contain characters from at least three of the following four classes: (i) English upper case letters, *A, B*, *C, etc.,* (ii) English lower case letters, *a, b*, c, etc. (iii) Westernized Arabic numerals, *0,1,2*, and (iv) Non-alphanumeric (special characters) such as punctuation symbols.
   d. Passwords may not contain your user name or any part of your full name.
   e. Passwords shall never be displayed, printed, or otherwise recorded in an unsecured manner.
5. Automatic log on scripts and other programmatic methods are not allowed.
6. Log on information is not to be shared with any other person.
7. Do not leave the workstation logged onto the network while away from their area. Users may elect to lock the workstation rather than logging off when leaving for very short time periods.
8. Only execute applications that pertain to their specific contract work.
9. Promptly report log on problems or any other computer errors to ITD at (904) 255-1818.
10. Promptly notify ITD at (904) 255-1818 if a breach of security or potential breach of security is suspected.
11. Users shall not install or use any type of encryption device or software on any City hardware, which has not been approved in writing by the Technology Security Group.
12. Do not attach any device to the City network without written approval from ITD.
13. Users may not remove any computer hardware from a City building for any reason, without prior written approval from ITD.
14. External users shall not delete, disable, or bypass any authorized encryption device, or anti-virus or other software program, installed on City hardware.
15. External users shall not attach any network or phone cables to any City device without written approval from ITD.
16. City data and/or software shall not be removed from a City Building without prior written approval from ITD.
17. Do not utilize City computer systems or networks for any of the following reasons:
    a. game playing,
    b. Internet surfing not required for their work activity,
    c. non-related work activity,
    d. any illegal activity, and
    e. Downloading files from the Internet.
18. External users are prohibited from intercepting or monitoring network traffic by any means, including the use of network sniffers, unless authorized in writing by ITD.
19. Users may not give out any City computer information to anyone.
20. All data storage media shall be erased or destroyed prior to disposal.
21. Do not remove or delete any computer software without the written approval of ITD.
22. Attempting to obtain or distribute City system or user passwords will result in immediate termination of access privileges.
23. External users shall not attempt to obtain or distribute door pass codes/passkeys or other access devices to secured rooms at any City facility for which they are not authorized.
24. All city-owned equipment issued to external users will be returned in the same condition as delivered.
25. City information technology services will not be used to send or receive threatening, obscene, abusive, sexually explicit language or pictures.
26. Usage of the interactive technology services must be legal under local, state, federal or international law. External users may not disclose of any private or confidential client information regardless of physical form or storage media (paper, computer, voice mail, microfiche, images, etc.). External users will not attempt to access not public data for personal purposes.
27. External users may not disclose of any private or confidential client information regardless of physical form or storage media (paper, computer, voice mail, microfiche, images, etc.). External users will not attempt to access not public data for personal purposes.

INFORMATION TECHNOLOGIES DIVISION

Jacksonville
Where Florida Begins.

Requesting User Information			
First Name:		**Phone:**	
Last Name:		**Email:**	
Position:			
Company:			
Address:			

By signing this form, you are bound to the terms of the External User Technology Use Agreement.
This authorization will expire in 12 months and must be renewed annually.

Signature:	
Print Name:	
Date: (mm/dd/yyyy)	

For use by authorizing party representing the City of Jacksonville

☐ **New COJ user login ID needed**		☐ **New VPN Client**	
☐ **Renewing existing COJ user login ID** **Print existing ID here:** _____		☐ **Renewing existing VPN Client login ID** **Print existing ID here:** _____	
☐ **Access need less than 12 months – please specify termination date**		**Termination Date:**	

As an authorized individual I allow this user to access City of Jacksonville technology services for 12 months. I understand this authorization must be renewed annually and responsible for requesting a renewal access at the end of account expiration date. One year from the above date external user signed on this agreement.

Print Name & Title:			
Signature:		**Date:**	

This user will require access to the following systems and/or applications:

1)		2)	
3)		4)	
5)		6)	
7)		8)	

Reason for Access (Notes):