

Grants Management

City of Bell
POLICY FOR GRANTS MANAGEMENT

Purpose

The purpose of this policy is to specify the circumstances when grant funding is appropriate and to clarify roles and responsibilities in internal grants management.

Policy

1. City departments shall actively pursue federal, state and other grant opportunities when deemed appropriate. Before accepting a grant, the City shall thoroughly analyze the implications of grant acceptance vis-à-vis the ongoing financial and operational implications that may be required.
2. Acceptance of all grants must be approved by action of the City Council. Said approval shall include authorization to appropriate funding to revenue and expenditure accounts.
3. The term of grant-funded employment positions shall be clearly identified and disclosed to the City Council for prior to approval. If the expiration of a grant requires the application of General Fund revenues for continued funding, this stipulation also must be disclosed.
4. Grant funding will be considered as a leverage of City funding sources. Inconsistent, one-time or fluctuating grant sources should not be used to fund ongoing programs.
5. Grants shall be accounted for in separate accounting funds.
6. The awarded City department assumes the lead role in grant management in collaboration with the Finance Department.

Department Responsibilities

City Department seeking and managing grant funding is responsible for:

- Preparation of grant application materials;
- Providing sufficient data to allow City Management to evaluate the costs and benefits of the proposed grant;
- Obtaining appropriate approvals for submission of grant, if necessary;
- Obtaining City Council approval for acceptance of grant;
- Understanding the operational and budgetary impact the grant has upon the City organization;
- Accumulating the appropriate accounting detail and supporting documentation;
- Preparation of reports required by the grantor;
- Providing the Finance Department with the following:
 - i. Grant Award Letter;
 - ii. Grant Contract;
 - iii. City Council minutes of action;
 - iv. Notice of Grant Award Form;
 - v. An administrative manual (this includes audit guidelines and programs, accounting procedures and administrative guides). This will enable the Accounting and Budget Departments to maintain grant files which are accurate and current.
- Providing copies of all grant amendments, program reporting, reimbursement requests and other communications to all agents involved in the grant administration process.

The Finance Department is responsible for:

- Assisting departments with any problems or questions regarding the grant submission process;
- Scheduling audit of grant programs when requested by Grantee Agency. City Staff will aid in the auditing process providing available source documents as requested by auditing agency;
- Coordinating the accounting for all receipts and disbursements related to the grant. Finance Department will determine setup and maintain the most appropriate method(s) of accounting for the grant in the financial system.

Technology

City of Bell
TECHNOLOGY USE POLICY

PURPOSE

The purpose of this administrative regulation is to provide guidelines for the appropriate use of all technology resources provided by the City. These resources include computers, servers, printers, scanners, software, Internet, Intranet, phones, and all other technology-related items. This regulation applies to anyone using or accessing the City of Bell network and other forms of technology.

1. Definitions.

- 1.1 Technology resources are provided to users of the City network for the purpose of conducting City-related business only. The use of City technology not specific to the mission or to the duties of the user as directed by the City is prohibited except as specified under section 3.10. This regulation is intended to supplement the City's personnel policies, such as the harassment policy that governs the rules of conduct and performance in the workplace.
- 1.2 All references to users in the context of this administrative regulation are assumed to include employees, contractors, volunteers, and others using City-provided technology.

2. General Policy/Procedure.

- 2.1 The use of City technology for personal profit or gain, or any other activity not specific to the mission or duties of the users or City is prohibited.
- 2.2 The use of City technology for an illegal, harassment, obscene, or other purpose, which could expose the City to liability or cause an adverse public perception, is prohibited.
- 2.3 The Information Technology contractor, under the direction of the Finance Director, has primary responsibility for the installation, management, and support of all technology resources.
- 2.4 All data and other forms of electronic information, including e-mail, that is stored on any type of media provided by the City are the City's. The City reserves the right to access and disclose all such stored information for any purpose.
- 2.5 Violation of any portion of the technology use regulation by any

user of the City computer network could result in loss of access rights and disciplinary action up to and including termination.

3. Computers and Network Use.

- 3.1 The Information Technology contractor will coordinate all computer service, equipment, additions, changes, moves, and repairs.
- 3.2 Unauthorized access, alteration, deletion, damage, infection, or destruction of any computer resource on the network is prohibited.
- 3.3 The Information Technology contractor maintains a standard configuration of computer hardware and software issued to users of the City network. Deviation by users from this standard configuration is prohibited. Changes to the system configuration must be requested from the Information Technology contractor.
- 3.4 Standard games, which are shipped and included in the operating system of each computer, will be allowed on City computers. Games used for services such as in the Community Services Department program are permitted. No other games will be allowed on systems. Standard games should only be accessed during employee break time. Any material found on a PC that does not directly relate to the job duties of the employee and/or the employee's department will be deleted.
- 3.5 Employees are encouraged to power off or place their computers or monitors into sleep-mode before leaving for an extended period of time (i.e., meetings, lunch, etc.). Equipment should not be left on overnight and should be completely powered off each evening.
- 3.6 Laptops issued to staff to be used for use while at the City should be stored in a locked or secured area.
- 3.7 The user is responsible for properly caring for the equipment while in his or her use. Do not mark on any equipment with pencil or pen for any reason. Do not permanently adhere any items to the monitors, keyboards, printers, mouse, or any other form of equipment provided to you. Keep all liquids and food away from the computer equipment at all times. Users are responsible for keeping the keyboards and monitors clean.
- 3.8 Report any problems with the equipment, software, or other computer-related problems to the Information Technology staff

immediately. Do not try to resolve any unfamiliar problems without their assistance. Do not answer any error messages on your screen if a problem occurs. If a problem does occur, please document what you were doing and when the problem started to facilitate Information Technology's staff assistance.

- 3.9 The City reserves the right to monitor all network traffic on the City network and to modify and/or restrict access if necessary.
- 3.10 The display of sexually explicit images, documents, or offensive material on any City system is a violation of the City's harassment policy. This includes sexually explicit or offensive material accessed from or received through the Internet, e-mail, or other electronic methods. In addition, sexually explicit or offensive material may not be archived, stored, distributed, edited, or recorded using any City resource.
- 3.11 Employees may occasionally use City resources during breaks for personal use, provided such use does not interfere with job performance, consume significant amounts of time, distract other employees, does not potentially cause discredit to the City, does not result in personal profit or gain, and is done in a professional and courteous manner. All other provisions of this regulation are in effect when resources are used for personal use.

4. Software Policy.

- 4.1 All software used on the City network must be acquired and licensed by the Information Technology contractor and the City of Bell. Software licenses and the physical media must be maintained in a central location by the Information Technology contractor.
- 4.2 Users may not copy City-licensed software or data to another system or media without prior approval of Information Technology contractor.
- 4.3 All software installation on any City resource must be installed or coordinated by Information Technology contractor. Users may not install any software onto any City-issued resource. All software must be evaluated for compatibility by the Information Technology contractor.
- 4.4 Any software, including databases, custom reports, graphics, or other work product developed while using a City resource or developed for use on the City network becomes the property of the City of Bell.

5. Security Policy.

- 5.1 All City network users are required to use personalized user IDs and passwords. The user ID will be assigned by the Information Technology contractor and follows the syntax of first name initial and full last name unless otherwise specified. The passwords are chosen by the user and are not known to the Information Technology contractor.
- 5.2 Passwords are confidential and should not be shared.
- 5.3 Passwords are used for logging into the City network, using applications, or accessing certain resources. Network passwords are set to expire every 90 days. The system will prompt users when a change is necessary. Users should choose a new password when prompted.
- 5.4 Passwords used should be unique and must adhere to the password policy in effect at time of password creation. The password policy will enforce duration and complexity.
- 5.5 Users of the City network are responsible for understanding and exercising reasonable security precautions. These precautions include, preserving the secrecy of user IDs and passwords, checking external data files for viruses before using on a computer, and deleting e-mails from unknown sources.
- 5.6 Because the City network is comprised of connected computers, servers, and other devices, access to other users' files may be possible. Users are expected to use caution and protect confidential data files when storing such data on network drives that are common areas to other users.
- 5.7 Virus protection software is resident on each computer. Users shall not disable this software.

6. Electronic Mail Policy.

- 6.1 Electronic mail is a method of communication not intended to replace written communication as part of a permanent file. Electronic communications necessary to be part of a permanent file should be sent as a word processing document attached to an e-mail and be printed and placed in the corresponding subject file in a timely fashion.
- 6.2 Confidential messages should not be placed on the electronic mail system.

- 6.3 Messages should be sent to smaller, rather than larger, audiences where appropriate. Limit the distribution list to those who need the information. Avoid broadcasting messages.
- 6.4 Limit the use of "high-priority" mail. Overuse may dilute the true urgency of future mail.
- 6.5 Users should use email auto reply when away from the office and will not be checking email remotely.
- 6.6 Be courteous with the use of Notify tunes.
- 6.7 Language that is insulting, offensive, disrespectful, demeaning, or sexually suggestive, will not be tolerated. Harassment of any form will not be tolerated. Sexual or ethnic slurs will not be tolerated. Obscenities or any representation of obscenities will not be tolerated.
- 6.8 Employees shall print communications necessary for file and then delete electronic mail and phone messages immediately after reading.
- 6.9 Users are prohibited from using the Electronic System to interfere with or disrupt other network users, services, or equipment or for direct personal gain. Disruptions include, but are not limited to, distribution of unsolicited advertising, the propagation of computer viruses, submission of large volumes of messages to other users or networks, and unauthorized entry to any other computer system.
- 6.10 All inbound and outbound e-mails and attachments are scanned for viruses. Any e-mails or attachments found to be suspect will be quarantined by automated software.

7. On-Line Services Policy.

- 7.1 The Internet is a rapidly evolving resource with a vast amount of information available through it. Internet resources are made available to City network users to improve communication and information exchange with citizens and others and to provide an informational and research tool.
- 7.2 The City employs internet filtering of certain websights and content. The City reserves the right and has the ability to view or access or disclose all such web access information for any purpose.

- 7.3 Users should only download files as they relate to their job function. Downloads can cause significant slowdown in the network response time, introduce viruses, or damage other systems and disrupt work for others. Users should not download any files that require installation without authorization from the Information Technology Division staff.
- 7.4 Knowingly generating, sending, requesting, receiving, or archiving any material which contains any comment or image that is discriminatory, offensive, defamatory, or harassing in nature is prohibited.
- 7.5 Use of chat rooms is prohibited.
- 7.6 Users shall not use any City resource to gain unauthorized access to other resources or entities. For example, a user with network access shall not attempt to gain access to areas on the City network or other outside networks.
- 7.7 Users should use caution when providing personal or business information over the Internet. Many sites collect this information for use in email Spam or for other fraudulent practices.
- 7.8 The City Manager shall determine appropriateness of materials posted to the Internet or Intranet.
- 7.9 The City of Bell permits the establishment of links from the City Internet website in conformance with this regulation. All links must be approved by the City Manager.
- 7.10 The City of Bell logo is a trademark of the City. Any use of the materials stored on the City's website is prohibited without the written permission of the City of Bell. The City of Bell retains all intellectual property rights including copyrights on all text, graphic images, and other content. Modification, distribution, mirroring, or use of images or other web content is prohibited.
- 7.11 The materials and information contained on or obtained from the City website are distributed and transmitted "as is" without warranties of any kind, either express or implied, including without limitation, warranties of title or implied warranties of merchantability or fitness for a particular purpose. Information contained on the City website, including information from external links thereon, is provided without any representation of any kind as to accuracy or content and should be verified by the user. The City of Bell is not responsible for any special, indirect incidental or consequential damages that may arise

from the use of or the inability to use the website and/or material contained on the site whether the material contained on the website is provided by the City or a third party.

8. Remote Access.

- 8.1 Access is available to the City network through remote access. This access includes e-mail service when a connection is established through a user's personal connection through his or her Internet Service Provider.
- 8.2 Remote access will be setup by the city's Information Technology contractor, and granted by the city through a secure "virtual private network" (VPN) connection only. Unless authorized by the City Manager, no employee shall use this ability to take the place of his or her attending work. However, it can be used in those instances when an individual may be off-site and needs to access the City network.
- 8.3 Access by outside agencies, temporary employees, project employees, interns, volunteers, probationary employees, or consultants is not permitted without specific approval of the City Manager.
- 8.4 All rules listed in this regulation apply when accessing the City network remotely.

9. Laptop Use.

- 9.1 Laptops may be assigned on a permanent basis to certain staff. All technology use rules apply to laptop users.