INFORMATION TECHNOLOGY POLICIES AND STANDARDS

INFORMATION TECHNOLOGY POLICIES & STANDARDS

REVISION HISTORY

REVISION	DATE OF RELEASE	SUMMARY OF CHANGES
Initial Release	August 1, 2012	-

INFORMATION TECHNOLOGY POLICIES & STANDARDS

TABLE OF CONTENTS

INFORMATION TECHNOLOGY POLICIES & STANDARDS

PURPOSE:

Information Technology Policies and Standards have been created to establish guidelines and best practices concerning access to and use of City-owned information technology (IT) resources. These Policies and Standards serve to enhance security and reliability of the City's information systems, thereby protecting vital information, improving communications, and ensuring continuity of operations in the event of an emergency.

SCOPE:

Information Technology Policies and Standards apply to all City employees who use the City's IT resources in the performance of their job duties ("employees"), as well as all other persons, such as employees of independent contractors, consultants, elected officials, appointed officials, volunteers, and other persons ("other users") who are authorized to use the City's IT resources in the performance of official City business. Employees and other users may be collectively referred to as "users".

GENERAL POLICY:

The City's IT resources, including all hardware, software, equipment, networks, and infrastructure, are provided for the exclusive purpose of conducting City business, enhancing efficiency and better serving the public interest. Management of these assets, as well as management of the City's IT consultants, is the responsibility of the Director of Financial Services. The City's IT consulting firm and/or its employees may be referred to as the City's "network administrator".

All messages, files, and user actions are subject to monitoring. No right of ownership or expectation of personal privacy is expressed or implied. City IT resources are not for personal use; users should refrain from using the City's IT resources for personal uses such as transmitting, saving, or storing personal files, photos, music or other data, sending and receiving personal email messages, or other non-work related internet activities.

Similarly, the City's phone system is designated for official City business and users should refrain from using the City's phone service for calls of a personal nature.

Electronic records and data should be handled the same as non-electronic records. All rules and procedures for public records requests apply to electronic records and data transmitted electronically.

Misuse of City IT assets will not be tolerated. Users are responsible for reporting known or suspected abuse incidents to their Department Director and/or to the Director of Financial Services. If an abuse incident potentially affects the City's IT infrastructure, the Director of Financial Services and the network administrator will take the actions necessary to secure the reliability and integrity of the infrastructure.

Consequences of inappropriate use or a violation of the City's IT policies may include revocation of a user's access to technology resources, disciplinary action leading up to and including termination, and/or legal action.

INFORMATION TECHNOLOGY POLICIES & STANDARDS

Included in this packet are the following Information Technology Policies and Standards:

Security and Infrastructure
Network Access and Use
Email Access and Use
Internet Access and Use
Access to Financial System
Synchronizing Smartphones & Tablet Devices to the City's Exchange Server

By signing this form, the user acknowledges these Information Technology Policies and Standards and that use of the City's IT assets constitutes acceptance of these terms.

User Name	Department
Signature	Date

INFORMATION TECHNOLOGY POLICIES & STANDARDS

SECURITY & INFRASTRUCTURE

POLICY

It is the policy of the City of Aliso Viejo to protect its IT infrastructure against disruption and maintain security of its data at all times.

The following policy provisions are adopted to ensure the internal and external integrity and security of the City's IT infrastructure:

1. Protection of centrally-managed or "citywide" IT assets is the responsibility of the Director of Financial Services in conjunction with the City's IT consultants. IT equipment will be recorded and assigned an inventory tag as required by the City's Fixed Asset Policy (Administrative Procedure 7).
2. Information must be protected according to its sensitivity, criticality and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed.
3. The Director of Financial Services shall oversee security features protecting the overall environment in conjunction with the City's IT consultants. Security features include, but are not limited to, the most current versions of anti-virus and anti-spyware software to protect against malware, viruses, Trojans, worms, spyware, adware, and other security threats and a firewall to control access to the City's network.
4. In the event of a security threat or other incident involving potential effects to the City's infrastructure, the Director of Financial Services and/or network administrator will take all actions necessary to secure the reliability and integrity of the infrastructure, including temporarily blocking or limiting users' access to the City's network and/or the internet to protect the City's IT assets (i.e. during a virus outbreak).
5. To ensure that City business objectives are met, all users have a responsibility to protect data from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional.

Disabling, removing, or overriding security features on a City-owned or networked computer constitutes a violation of this Security Policy.

INFORMATION TECHNOLOGY POLICIES & STANDARDS

NETWORK ACCESS AND USE

POLICY

The City of Aliso Viejo has undertaken significant efforts to implement an information sharing infrastructure to meet the business needs of the City, the work requirements of users, and the communication needs of the public. This policy serves to protect that infrastructure and the business needs of the City and its citizens.

The following policy provisions are adopted to ensure the internal and external integrity and protection of the City's networks:

1. No non-City owned platforms (PCs, laptops, Smartphones, tablets, or any other device capable of connecting to the City's network) will be directly connected through any means to the City's networks, without the pre-approval of the Director of Financial Services or network administrator.
2. Users are responsible for seeking the approval of the Director of Financial Services for equipment and devices that require network access *prior to* attempting to connect to the network.
3. No remote connectivity or remote control software (e.g. PC Anywhere, GoToMyPC, etc.) will be used to connect to the City's network in any way unless approved in advance by the Director of Financial Services or network administrator.
4. All platforms approved by the Director of Financial Services for connection to the City's networks will have been proven to be free of any viruses, spyware, and/or other security threats. Once connected, the City's minimum anti-virus protection software standards will apply.
5. Access to the City's network is granted by the network administrator. Each user is provided a username and password, for that individual's sole use, which is tied to the user's unique account profile and Exchange account. Users shall not allow someone else to use their account and/or password. Network users are responsible for activity on their individual accounts and shall be held liable if someone else uses their account and violates this policy.

Unauthorized access or use of the City's Network System constitutes a violation of this policy.

INFORMATION TECHNOLOGY POLICIES & STANDARDS

EMAIL ACCESS AND USE

POLICY

Users are allowed access to City email services from City-owned or networked computers for purposes of communication, research and other work-related activities. All existing laws and City policies apply to users' conduct when using City email services regardless of whether using the services on a City-networked computer, through Outlook Web Access, or on a synchronized wireless device such as a Smartphone or tablet.

The following policy provisions are adopted to ensure appropriate access and use of the City's email services:

1. The City of Aliso Viejo is the owner of all email accounts and addresses in its registered domains. All email messages processed by the City's email server become the property of the City of Aliso Viejo. City of Aliso Viejo email users have no right of ownership or expectation of personal privacy in their email usage.
2. City email services shall be used in accordance with all applicable Federal and State laws, City ordinances, policies, and standards of conduct. All users of City email services are expected to conduct themselves in a professional and ethical manner.
3. City email services are provided to users solely for the purposes of conducting City business.
4. Offensive content may not be transmitted, displayed, archived, stored, distributed, edited, or recorded using City email resources. Offensive content includes, but is not limited to, pornography, sexual comments or images, profanity, racial slurs, gender-specific comments, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability, veteran status or any protected status of an individual or that individual's relatives or associates. Any content that may be interpreted as libelous, defamatory, or slanderous is prohibited.
5. Users are authorized to access, use, modify, copy, or delete files and data on their own accounts only. Users should not perform any functions on another user's email account without prior authorization. Users should use caution when allowing someone else to use their account and/or password. City email users are responsible for their email accounts and will be held accountable if someone else uses their service with permission and violates this policy.
6. City email users should only use City IT resources (i.e., City email services) to send and receive email messages while conducting official City business. A City email account may be requested for any contract employee, consultant, or other person working on behalf of the City and conducting official City business.
7. City email users may not automatically forward email messages received at a City email address to any personal or non-City email account(s) or address(es). Similarly, City email users shall not automatically forward email messages from personal or non-City email accounts to a City email account or address.
8. Subscriptions to mailing lists, "listservs," or other mass mailings are authorized only when used to conduct official City business. Non-work-related subscriptions to mass mailings are

prohibited. The City reserves the right to unsubscribe any or all City email addresses from said mailings.

9. To maintain reasonable storage limits, City email users are required to archive email messages older than six months and permanently delete archived messages older than one year. The Network Administrator will set these archive rules for each user. If a user determines an email should be saved beyond one year, it is the user's responsibility to save the email in a location other than the Exchange server.
10. A file sharing account can be used to transfer large files that are beyond the capacity of the City's regular email system or recipient's email system. Files uploaded to a file sharing account should be *private until shared*.
11. The City reserves the right to inspect any email message processed through its email server. Software installed on the City's email server provides for anti-spam and anti-virus protection. Email messages the City deems unsolicited, inappropriate, objectionable, harassing, deceptive, prohibited by City policies or standards, or unrelated to the conduct of the official business of the City may be returned, rejected, or discarded in an attempt to limit the amount of unsolicited or bulk emails processed by the City's server. Network Administrators will make reasonable efforts to ensure that legitimate email messages are not refused.
12. The City reserves the right to limit or restrict any user's email usage to one gigabyte (1 GB).
13. Access to City email services shall be immediately and permanently revoked upon employee termination or retirement. The City will forward email messages addressed to terminated or retired City employees to other City email addresses. The City shall not provide address verification, correction or forwarding to personal or non-City email accounts or addresses under any circumstances.

Unauthorized access or use of City email services constitutes a violation of this policy.

INFORMATION TECHNOLOGY POLICIES & STANDARDS

INTERNET ACCESS AND USE

POLICY

Users are allowed access to the Internet from City-owned or networked computers for purposes of communication, research, procurement, and other work-related activities. All existing laws and City policies apply to users' conduct when accessing the Internet on City-owned or networked computers. City equipment should not be utilized to view unethical sites. Internet users are responsible for ensuring their internet use is effective, ethical, productive, and lawful.

The following policy provisions are adopted to ensure appropriate access and use of the internet while using City resources:

1. Internet access is provided to users for the purpose of conducting official City business.
2. Each user of the City's internet service shall identify themselves accurately and completely when corresponding or participating in online activities.
3. City internet facilities and computing resources must not be used to knowingly violate the laws and regulations of any Federal, state, city, or local jurisdiction in any way.
4. Users have no right of ownership or expectation of personal privacy as to their City internet usage. It is possible to monitor internet usage, and the City reserves the right to inspect any and all network traffic and files stored on City resources. The City reserves the right to limit or restrict any user's internet usage.
5. Internet access from the City's networks may be "filtered" using a third-party product or service, at the discretion of the City Manager and/or Director of Financial Services, to limit or block access to certain sites deemed unnecessary for the conduct of official City business. The network administrator may temporarily block or limit access on an emergency basis to protect the City's information technology assets (i.e., during a virus outbreak).
6. Offensive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using City network, printing or computing resources. Offensive content includes, but is not limited to, pornography, sexual comments or images, profanity, racial slurs, gender-specific comments, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability, veteran status or any protected status of an individual or that individual's relatives or associates. Any content that may be interpreted as libelous, defamatory, or slanderous is prohibited.
7. City internet access shall not be used to conduct personal business and/or any activity for personal gain, gamble, run a business, conduct political activities, or take part in any prohibited or illegal activity.
8. Users may not use City internet access to post a message to an internet message board, chat room, "weblog", "listserv", or other internet communication facility, except in the conduct of official City business. The message must clearly identify the author by name, his or her title or role within the City (i.e. employee position, contract staff position, etc.) and provide an official return City email address or phone number for contact. Any opinions expressed must include a disclaimer stating that the opinions are those of the author and not necessarily those of the City of Aliso Viejo, its officers or employees.

9. Nothing in this policy shall be construed as requiring the City to provide any technical resources or assistance in support of any internet use which is not directly related to the conduct of official City business.
10. Users may not use City resources to download or distribute software programs or applications. Only the City's network administrator may download, add, or change software and applications on City-owned IT equipment. Software, files or content downloaded via the City's internet service provider may only be used in ways consistent with all applicable laws, regulations, licenses, copyrights, and City policies.
11. Peer-to-Peer or file-sharing internet-based applications are strictly prohibited and should not be downloaded or accessed using the City's internet service. These applications are known to also download "spyware" and "adware" programs in addition to opening up the City's network security infrastructure to viruses, worms, and other security threats.
12. The online streaming of media unrelated to City business is not condoned due to interference with the City's bandwidth capacity, internet speeds, and/or network security.
13. No user may install, remove, or otherwise modify any hardware or software for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security measures the City may have in place.
14. Use of the internet must not disrupt the operation of the City network or the networks of other users, nor should internet use interfere with productivity.

Unauthorized access or use of the internet using City resources constitutes a violation of this policy.

INFORMATION TECHNOLOGY POLICIES & STANDARDS

ACCESS TO FINANCIAL SYSTEM

POLICY

This policy serves to limit the City of Aliso Viejo's exposure to fraud and theft of its assets by ensuring its financial systems are accessed only by authorized personnel.

The following policy provisions are adopted to ensure the security and integrity of the City's Financial System:

1. The City will take all steps possible and practical to restrict access to the financial system that processes financial or monetary transactions to limit the opportunity for theft or fraud. This includes, but is not limited to, transactions involving purchase orders, accounts payable, accounts receivable, fixed assets, and all entries to the general ledger.
2. All users are allowed access to the City's financial system with read-only rights. Specific users are then granted access to particular modules as determined by their job functions, but without the authority to post changes, additions, deletions, revisions, or updates to the financial system.
3. The Director of Financial Services has the discretion to allow temporary employees access to the financial system, for purposes of data entry only, and under the responsibility of the Accountants and Director of Financial Services.
4. The Director of Financial Services is required to approve and post all transactions to the financial system, thus ensuring proper segregation of duties to meet generally accepted accounting and auditing standards.

Unauthorized access or use of the City's Financial System constitutes a violation of this policy.

INFORMATION TECHNOLOGY POLICIES & STANDARDS

SYNCHRONIZING SMARTPHONES AND TABLET DEVICES TO THE CITY'S EXCHANGE SERVER

POLICY

This policy serves to define the circumstances under which users may wirelessly synchronize personal or non-City owned Smartphones or tablet devices with the City of Aliso Viejo's Microsoft Exchange server.

The following policy provisions are adopted to ensure appropriate access and use of the City's exchange server while using personal or non-City owned devices:

1. Users are responsible for seeking the approval of the Director of Financial Services *prior to* synchronizing wireless devices with the City's exchange server to ensure the devices being used are compatible with the City's infrastructure and also to maintain the listing of users synchronizing their personal devices should it be needed in the event of a security threat or breach.
2. Only compatible devices will be approved for wireless connection and synchronization. Compatible devices are determined by the City's network administrator and can be found in Exhibit A – Equipment and Software Standards.
3. Upon approval, users will be assisted with the initial set up of the City's exchange server on their personal device. Nothing in this policy shall be construed as requiring the City to provide any technical resources or assistance in support of any personally owned device beyond set up of the Exchange account.
4. Personal Smartphone and tablet devices synchronizing to City email servers will be allowable provided no additional licensing expense or service administration is required to enable the device. The City assumes no liability for non-City owned devices.
5. Any and all existing City Ordinances, Administrative policies, and/or Departmental policies shall apply to the use of personal Smartphone and tablet devices synchronized with the City's exchange server.
6. The owner of the device is responsible for enabling security features on the device, including passwords and SSL data encryption. Should the device be lost or stolen, confidentiality of data is of utmost importance to the City and any compromised data will be the responsibility of the owner.

Unauthorized access to or use of the City's Exchange server constitutes a violation of this policy.

EQUIPMENT AND SOFTWARE STANDARDS

POLICY

The following standards apply to all computers, computer-related equipment, and software purchased, owned, or maintained by the City of Aliso Viejo. Additionally, these minimum standards apply to any computers or computer-related equipment owned or operated by other users who have been authorized to connect to the City's networks in the performance of official City business.

These standards serve to ensure equipment compatibility within the broader infrastructure as well as to mitigate the costs of setup, training, and oversight. These standards are intended to satisfy the requirements of conducting daily business in an efficient manner as well as to achieve substantial cost savings in training and support in addition to the advantages of volume purchase discounts.

All software will be purchased by the Department of Financial Services. Training sessions will be provided for all users upon a significant software upgrade or migration.

STANDARDS

Preferred Server Operating System:

Per the City's IT Strategic Plan, server operating systems will be updated as necessary to keep pace with current standards and supported versions.

Preferred Backup & Replication Software:

Backup Exec Remote
Backup Exec 12.0

Minimum Configurations for New Desktop/Notebook/Tablet Computers:

Intel Core 2 duo 2.4 GHz processor or faster (Core i5 or i7 are acceptable)
Windows 7 Professional
4 GB DDR2 SDRAM 667 MHz or faster
DVD-ROM/CD-RW
4 or greater USB ports
100GB (or greater) SATA 2 7200RPM or faster hard drive
Integrated or PCI Express Video Card
Integrated or PCI Sound Card
17" or larger monitor
USB keyboard and optical USB mouse
3-Year hardware maintenance

Supported Operating Systems:

Windows 7 Professional (Preferred) and Windows XP Professional

Supported Software:

Microsoft Office 2010 Professional (Preferred), 2007 Professional, and 2003 Professional

Adobe Acrobat X Professional
Adobe Reader 9.0
Microsoft Internet Explorer 8.0
INCODE
Adobe Photoshop CS5
Mozilla Firefox
Google Chrome
Java Platform SE 6 U31

Software by Contract Vendors:

FileMaker Pro
Laserfiche 8.0
Digital Maps

Compatible Smartphone/Tablet Devices:

Apple iPhone and iPad
Windows Phone 7 and other models using Windows Mobile Operating System
Nokia E-series phones with Mail for Exchange
Android Smartphones and other models using the Android Operating System
Other devices as approved by the network administrator

Required Anti-Virus and Anti-Spam Software:

Symantec or others as approved by the network administrator

Maximum Mailbox Size Limit:

1 gigabyte (GB)

Email Message Size Limit:

Internal Emails – Unlimited
External recipients – usually 10 MB due to the standards of most internet providers and/or recipient email systems.

THIN CLIENTS AND THE VIRTUALIZED ENVIRONMENT

The set-up of a thin client machine is different from a traditional desktop or laptop because you are now working from a virtual server. The physical thin client does not have an internal hard drive as normal computers do. Instead, there is a small chip embedded with the Microsoft Windows 7 program that connects the user to the virtual server where all programs and data are stored.

Logging On

When you turn on your thin client, you will see the "Windows 7 Embedded" logo at the bottom of the desktop. This is the basic Windows program embedded on the thin client that you will use to connect to the Windows 7 program on the server. Click the icon on the desktop to connect to the Windows 7 Enterprise server.

Enter your username and password to connect to the Windows 7 Enterprise server. You will now be working off the server. The Windows 7 Enterprise logo will be at the bottom of the desktop. You will notice the system is much faster! This is due to your program files being stored on the server instead of a smaller, slower computer processor.

Logging Off

To log off the Windows 7 Enterprise server, you must key Ctrl+Alt+**Insert** instead of Ctrl+Alt+**Delete** (which logs off the thin client machine but not the virtual server). It is important to log off the virtual server (Windows 7 Enterprise) as it disconnects your profile.

If you ever do accidentally select Ctrl+Alt+Del and log off the thin client machine (instead of Ctrl+Alt+Ins), you will be stuck at the Windows "Embedded" screen and will not be able to log on using your username and password. Instead, you must sign into Windows "Embedded" with the Username "User" and password "User" (both with a capital U). You should then be back to the Windows Enterprise screen where you can log on to the Enterprise server with your usual username and password.

Downloads

On a virtualized environment, programs can only be added by the network administrator. Therefore, users are unable to save downloaded programs. Upon logging off, any unauthorized programs are automatically deleted by the system.

Saving Files

Users are encouraged to save files to either the share drive (S:\), personal drive (H:\), or Public Works drive (P:\). Saving files to these locations will ensure the data is backed up and secure.