PURPOSE

The purpose of this Policy is to ensure that the Company’s information technology resources are used 1) for business purposes consistent with the mission of the Company, 2) in accordance with Company policies, procedures, and contractual obligations, and 3) in compliance with applicable laws and regulations. It is intended to protect both the Company and users from possible liability and to safeguard Company assets and information. It applies to all users of Tetra Tech’s information technology resources. Users may be employees, clients, contractors, teaming partners, or suppliers of Tetra Tech and its subsidiaries and affiliated companies worldwide.

ACKNOWLEDGEMENT

All employees will acknowledge acceptance of this policy as required by Tetra Tech.

If a non-employee requires access to the Company’s information technology resources, it is the responsibility of the Tetra Tech employee who engages those services to provide the individual with a copy of this policy and to require they sign the acknowledgement located on the last page of this form. The signed acknowledgment, approved by management, should be given to the local IT representative before access rights to networks or systems are granted. Failure to acknowledge this policy may result in the revocation or suspension of a user’s computer credentials.

For questions regarding the Acceptable Use Policy, contact your Business Group IT Director or Corporate IT.

POLICY

Use of Company computers, networks, messaging systems, and internet access is a privilege that may be revoked at any time for inappropriate conduct. Users are expected to act responsibly and to respect others. Examples of inappropriate conduct include, but are not limited to, the following:

- Engaging in private, personal, or outside business activities;
- Promoting non-Company related causes;
- Misrepresenting oneself or the Company;
- Engaging in unlawful or malicious activities;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in any message;
- Accessing, sending, receiving, storing, or printing pornographic, racist, sexist, or otherwise discriminatory, or objectionable materials;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Infringing in any way on the copyrights or trademark rights of others;
- Unauthorized or unlicensed use of software or intellectual property;
- Knowingly propagating or disseminating malicious software of any type;
- Using recreational games or gambling;
- Use of peer-2-peer file sharing applications;
- Defeating or attempting to defeat security restrictions on Company systems and applications.

Use that interferes with normal job functions or the ability of users to perform daily job activities is also considered inappropriate. This Policy informs users that the tools, applications, and information created and accessed from the Company’s computer systems are the property of Tetra Tech, and users should have no expectation of privacy on Company-owned and Company-administered systems.

Antivirus and other similar client security agents adopted for use by the Company are mandatory on all Company computers. They may not be removed or disabled without permission from IT management.

Users must not password protect or encrypt company communications or company data unless authorized by management to do so.
Monitoring: Tetra Tech provides the network, Internet, computers, electronic messaging, and other Information Technology resources for the conduct of Company business. Company IT resources are subject to monitoring, logging, auditing, and inspection at the Company’s discretion. Data and correspondence stored on company systems may be subject to legal and administrative inquiry. Tetra Tech may inspect any information stored on its systems at any time without notice.

Passwords: Initial passwords are assigned by the IT department. Users must change their initial passwords as soon as possible using the instructions provided by IT. Users will also be required to change their passwords on a regular basis by Company Policy. Passwords must not be shared, stored, or displayed in locations where they could be accessible to others. Sharing your own password or using another person’s password is prohibited. Tetra Tech reserves the right to override any employee-selected passwords or codes.

Electronic Messaging: The content of all electronic messages is governed by the Company’s employee manual and Code of Conduct. E-mail and other means of electronic communication should be used for appropriate business purposes. Messages should be treated as confidential by other users and accessed only by the intended recipient. Users are not authorized to retrieve or read any e-mail messages that are not sent to them.

In order to provide a complete and secure record of all Company correspondence, Company related electronic messaging must be performed on Tetra Tech’s messaging systems. Users must not auto-forward e-mail outside of the Tetra Tech e-mail system or forward business-related correspondence to personal e-mail accounts. Public email systems and instant messaging programs, such as AOL Instant Messenger, Windows Live Messenger, Yahoo Messenger, etc. are not supported by the Company and may pose security risks. Use of non-Company messaging systems for Company correspondence must be approved by the Group President and CIO.

Network Security: Users are prohibited from any attempt to alter or breach the Company’s security systems. To safeguard network security and performance, no device or network service such as computers, printers, scanners, routers, hubs, sniffers, web-cams, wireless access points, or other IT-related technologies may be placed on the network without approval of the IT. Access rights to company systems and applications, including email, will be discontinued upon termination, or when an employee’s status becomes inactive.

Remote Access: Remote access to the Company network must be accomplished over an encrypted VPN connection using a Company-provided VPN client, or secure connection facilities (e.g. SSL Citrix, 128-bit encrypted Terminal Server) as approved by the IT Security Director. Unencrypted connections using terminal server, remote desktop, PcAnywhere, telnet, and other similar technologies are not permitted unless they traverse an already-established VPN connection.

Physical Security: Access to computer rooms will be limited to IT staff members who require access for the normal performance of their jobs.

Care of Equipment: Users are responsible for the care and protection of the equipment issued to them. Employees will not deface or physically alter Company-provided equipment. Users must return all equipment to the Company upon completion of the assignment for which it is intended, at termination, or at the request of management or IT personnel. Equipment issued solely for use at home or other non-business location must be approved in advance by management and IT and a record of the equipment maintained by IT.

Company-Owned Equipment: Company equipment is meant to be used by authorized personnel for Company business. Equipment must adhere to established standards and not be altered in any way that would compromise the integrity of the systems, data, or security. Where Company equipment is used on client-owned premises or connected to client-owned systems and networks, it is also subject to client policies relating to equipment use. In the event that there is a conflict between the Company’s Acceptable Use Policy and that of a client’s, the more restrictive policy will prevail.
Non-Company Owned Equipment: Non-company owned equipment includes personal computers, laptops, personal digital assistants, digital cameras, modems, wireless access points, USB hard drives, flash cards, storage devices, etc.

Employees are discouraged from using personally owned equipment for Company business. The Company is not responsible for the security, maintenance, or protection of personal equipment.

Visitors may connect computers to Tetra Tech’s guest wireless network for firewalled internet access only. Equipment owned by clients, contractors, teaming partners, or suppliers may only be connected to Company systems or networks with prior authorization of IT.

Non-Company owned equipment attached to Company networks or systems is subject to inspection by authorized Tetra Tech IT staff. Company information stored on this equipment remains the property of the Company. It is subject to the Company’s policies on confidentiality, may be subject to inspections by the Company, and must be removed at the Company’s request. Non-Company owned equipment may be disconnected from Company-systems and Company owned information removed without the permission of or notice to the user.

Internet Use: Internet access is provided to users for business purposes. Any personal use should be incidental and should not interfere with the performance of an individual’s job function. Users with internet access are expressly prohibited from accessing, viewing, downloading, uploading or printing violent, pornographic, sexually explicit, or other materials that may be considered offensive, as outlined elsewhere in this policy. In addition, users should be mindful that there is no assurance that e-mail text, attachments, or other Company information sent or posted within the Company and on the internet will not be seen, accessed, or intercepted by unauthorized parties.

Social Networking: This includes blogging, chat rooms, forums, social sites, etc. Company systems should not be used for personal networking. Company sponsored blogs require the approval of your Group President and CIO. Company related blogs must follow these guidelines:

1. Identify your name and position with the Company;
2. Don’t break news, and don’t disclose confidential information of the Company, its suppliers, customers, or partners;
3. Avoid posting personal information;
4. Use Company disclaimers to avoid misrepresentation;
5. Speak for yourself;
6. Consider the reactions of others before you post.

Software Usage: Users are expected to use Company-authorized and provided software. All software is to be used in accordance with the terms of the applicable software licenses. In order to protect the integrity and security of the Company’s systems, users are not permitted to install applications, demos, or upgrades without the prior approval of their manager or their IT department. Software purchased by the Company shall not be installed on employee-owned or other third-party computers unless those installations are authorized by Company management, and then only after the appropriate licenses are procured. Conversely, employee owned software must not be installed on company owned computers.

Addenda: Policy applicable to a specific region or country will be addressed in addenda.

Addendum A – Canada’s Personal Information Protection and Electronic Documents Act for Tetra Tech companies located in Canada.
CONSEQUENCES OF VIOLATION

Failure to comply with this policy governing the use of IT resources may result in consequences which could include the revocation of user access and privileges, removal of equipment, employee discipline up to and including termination, and possible civil or criminal penalties.
Acceptable Use Policy Acknowledgment Form

After reading this policy, please sign the coverage form and submit it to your facility’s IT department for filing.

By signing below, the individual requesting Company computer and/or network access hereby acknowledges receipt of and compliance with the Acceptable Use Policy. Where this policy references outside policies (i.e. Employee Handbook), it is the responsibility of the user to request copies of the appropriate policy. Furthermore, the undersigned also acknowledges that he/she has read and understands this policy before signing this form.

Computer and/or system access will not be granted until this acknowledgment form is signed by the individual. After completion, the form is filed in the individual’s human resources file (for permanent employees), or in a file specifically dedicated to Acceptable Use Policy Forms (for contract workers, etc.), and maintained by the IT Department. These acknowledgment forms are subject to internal audit.

Location: __________________________________________________________

Business Purpose: ______________________________________________________

Name: _______________________________________________________________

Employee: □ Vendor/Supplier: □ Contractor or Other: □

Requestor Signature: __________________________________ Date: ___/___/_____

Manager Approval: __________________________________ Date: ___/___/_____
