Procurement Card Internet Purchase Guidelines

Recommended Guidelines and Information for State Employees using the Internet for Purchases:

1. **Know with whom you are dealing.**
Before doing business with a company, research the legitimacy of the company. Identify the company's name, the physical address, and an e-mail address or telephone number, so you can contact the company with questions or problems. Consider dealing only with vendors that clearly state their company's buying policies. Is the company affiliated with industry groups, seal programs or other self-regulatory programs you trust? For example, the Better Business Bureau offers a web site reliability seal.

"Websites carrying the BBB*OnLine* Reliability seal are all members of their local Better Business Bureau, have been in business for at least one year, have agreed to abide by BBB standards of truth in advertising, and have committed to work with the BBB to resolve consumer disputes that arise over goods or services promoted or advertised on their site. Use the following URL site for further information and to review the full BBB*OnLine* Reliability standards that companies meet. http://www.bbbonline.com/

2. **Know what you are buying.**
Look for accurate, clear and easily accessible information about the goods or services being offered by the company. If you have any questions regarding the product or the service, contact the company and get answers **before** you place an order.

3. **Understand the terms, conditions and costs involved in the sale.**
Find out up front what you're getting for your money-and what you're not. Get a full, itemized list of costs involved in the sale, terms of delivery or performance, terms and conditions, and methods of payment. Do these terms and conditions conflict with State of Colorado Terms and Conditions? Confirm with the Internet company that the State does not pay sales tax and provide the tax-exempt number to the company. This might require a telephone call to the company. The State of Colorado tax-exempt number is 98-02565.

   Look for information about restrictions, limitations or conditions of the purchase; instructions for proper use of products, including safety and health care warnings; warranties and guarantees; cancellation or refund policies; and the availability of after-sale service.

   Remember that under the fiscal rules, all purchases for goods and services costing over $3,000 must be done using a PO or state contract. Your agency may have more restrictive thresholds.

4. **What recourse is available if there are problems with the purchase?**
Do business only with companies that state their commitment to customer

satisfaction. Deal with companies that promise to resolve consumer complaints or difficulties quickly and fairly, without imposing excessive charges or inconvenience. (Some companies charge restocking fees for returned merchandise.)

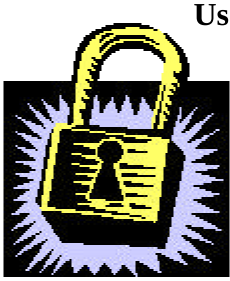
5. **Keep your Privacy private.**
   All businesses require information about you to process an order. Some use it to tell customers about products, services or promotions, but others share or sell the information to other vendors. This may be a practice that you may not be comfortable with and you may decide not to do business with that particular vendor.

6. **Protect yourself when paying online.**
   Look for information posted online that describes the company's security policies, and check whether the web site is secure and encrypts your personal and financial information during online transmission. Don't knowingly allow web sites to save your procurement card number for future use. See the section titled **Secure Transmissions on the Internet** below.

7. **Maintain security and privacy on your end.** Don't share your procurement card. Don't share online accounts. Keep your password(s) private. Be creative when you establish a password, and never give it to anyone. Avoid using a telephone number, birth date, or a portion of your Social Security number. Instead, use a combination of number, letters, and symbols. Don't save your password to your computer.

8. **Keep records of the purchase request and confirmation receipt**. Write down additional information as appropriate. There can never be too much documentation.

Secure Transmissions on the Internet



Use a secure WEB browser. Information can be "sniffed" as it is transmitted over the Internet. If a transmission is not secure, then others could obtain sensitive information such as procurement card numbers without the owner being aware that the card number has been compromised. Technology such as Secure Socket Layer (SSL) can be used to encrypt the data while it is being transmitted

Most modern web browsers, Netscape and Internet explorer, are able to use SSL to send encrypted data to a web site. But the web site must also be using SSL for the particular page that contains the sensitive data. Below, are the guidelines for you to use to determine whether or not the web site is secure.

Addressing Web Site Security

Only buy at secure sites. The web site computer should use SSL to communicate with your web browser. You often can tell when you have reached a secure page on a web site because you will see a pop-up notice in your browser, and/or see an icon of a locked lock at the bottom of the browser. You may also look for the HTTPS vs. just HTTP at the start of the address line for the page. These abbreviations indicate how the information is being transmitted and the S in this case means it is secured using Secure Socket Layer.

If the above indications are not present on the browser window, try right clicking on a blank part of the web page near the data that should be securely transmitted. On the menu that appears, select the 'View Frame Info' (Netscape) or 'Properties' (MS Internet Explorer) option. In the information that is displayed, look for an indication that SSL is being used or that the web page is secure or private. Look for a sentence to that effect.

If there is no indication of such security on the web site, don't buy from that site. If you are suspicious that a web site that state employees are buying from is not trustworthy or is lax in security, don't order from that site and report it to the State Purchasing Office at 303-866-6100.

Additional Information About Internet Security

Web sites for further reading are listed below:

http://www.techtv.com/callforhelp/projects/story/0,23008,2232583,00.html
http://www.ftc.gov/index.html
http://www.ftc.gov/bcp/conline/pubs/online/sitesee/index.html
http://www.bbbonline.com/
http://www.bbbonline.com/consumer/index.asp
http://www.extension.iastate.edu/Publications/PM1789G.pdf
http://shoppingguide.hypermart.net/safety.html

Glossary

Certificate. See digital certificate.

Certificate authority. A private company that issues digital certificates.

cookie. A "cookie" is a small text file that a website can place on your computer's hard drive in order, for example, to collect information about your activities on the site or to make it possible for you to use an online "shopping cart" to keep track of items you wish to purchase. The cookie transmits this information back to the Web site's computer, which, generally speaking, is the only computer that can read it. Most consumers do not know that "cookies" are being placed on their computers when they visit websites. If you want to know when this happens, or to prevent it from happening, you can set your browser to warn you when a website attempts to place a "cookie" on your computer. Please note that you will not be able to shop at certain web site unless you agree to cookies.

cryptography. The conversion of data into code for transmission over a network.. The original data is converted into code using an encryption algorithm, and is decoded (decrypted) at the receiving end.

The encryption algorithm uses a key, usually a binary number 40 to 128 bits in length. The key is mathematically combined with the data itself to create the code. At the receiving end, the key is used to "unlock" the code, restoring the original data.

Traditionally, encryption uses a secret key which both the sender and receiver use. This is the fastest method, but transmitting the secret key to the recipient is not secure.

A second method, public key cryptography, is now used in secure Internet communication. Each recipient has a secret private key, and a public key that is published. The sender looks up the recipient's public key and uses it to encrypt the message, and the recipient uses the private key to decrypt the message. There is never any need to share the private keys, so they are never in transit and are not vulnerable to being discovered by unauthorized parties.

digital certificate. The electronic equivalent of an ID card, used in conjunction with a public key encryption system. Also called digital IDs, digital passports, X.509 certificates, or public key certificates.

A digital certificate is an owner's public key, which a certificate authority has digitally signed. Certificate authorities (CAs) such as VeriSign Inc., issue a digital certificate to an individual or business after verifying the identity of that individual or business. The certification process varies depending on the certificate authority and the level of certification. The process may require identification such as drivers licenses, notarization, or fingerprints.

A person sends a digital certificate along with an encrypted message, to show that the sender is truly who he or she claims to be. The recipient uses the certificate authority's public key, which is widely publicized, to decrypt the sender's public key attached to the message. The sender's public key is then used to decrypt the actual message.

digital signatures. Digital signatures work just like paper-and-ink signatures, allowing document recipients to confirm the source of a document. Digital signatures are generated by using digital certificates.

encryption. A method of encoding data for security purposes. 128-bit encryption is much more secure than 40-bit encryption. See also cryptography.

extranet. A web site that an Internet business creates for existing customers. An extranet can provide access to research, databases, or any other information that is not publicly available. An extranet uses the public Internet to transmit the information to its users, but requires a password to gain access.

fire wall. A method for keeping a local area network secure. A firewall separates a company or organization's public web server from its internal network, so employees or members can use the public Internet but the public cannot gain access to the company's internal documents.

intranet. A company or organization's internal web site that can be accessed only by employees or members. An intranet cannot be accessed by the general public. See fire wall.

key. A numeric code that is combined with data to encrypt (encode) the data for security purposes. See cryptography.

privacy policy. A statement included at a web site that explains to visitors the web site's policy about collecting and disseminating information about individuals.

public key. The published part of a public key cryptography system. The private part is known only to the owner. See cryptography.

public key cryptography. See cryptography.

public key infrastructure (PKI). A policy that establishes a secure method for exchanging information within an organization, industry, or country. PKI includes cryptography, the use of digital certificates and certificate authorities, and the system for managing the process.

SSL (Secure Sockets Layer). The leading security protocol for the Internet, developed by Netscape. When a user navigates to a secure site on the Web, his or her browser sends its public key to the site so the site's server can securely send a secret key to the browser. The browser and server are then able to exchange data using secret key encryption. SSL has been combined with other protocols and authentication methods into a new protocol known as Transport Layer Security (TLS). Secure Socket Layer may use one of two levels of encryption: 40-bit and 128-bit. With 40-bit encryption, there are billions of possible keys to decipher the coded information, and only one of them works. Someone intercepting the information would have to find the right key - a nearly impossible task. With 128-bit encryption, there are 300 billion trillion times as many keys as with 40-bit encryption. It is virtually impossible for an unauthorized party to find the right key, even if they are equipped with the best computers.

Trojan horse. A program that appears valid, but when activated performs unauthorized activity. Such a program can be used to locate a person's password, or make a computer vulnerable to future illicit entry. A Trojan horse can also simply destroy programs or data on the person's computer. A Trojan horse is similar to a virus, except that it does not replicate itself. See virus.

virus. Software used to infect a computer. A virus is concealed by burying it inside an existing program. Once a person runs the program, the virus is activated. The virus then replicates itself and attaches copies of itself to other programs on the computer.

Viruses can be simple pranks (such as a rude message that pops up on the screen unexpectedly), but they can also destroy programs and data either immediately or at a scheduled time (including months or years later).

Warning: A virus can be attached to a data file such as an email message, as well as other kinds of programs.