2001

WebTrust program : confidentiality principle and criteria, Version 3.0, June 15, 2001; Exposure draft (American Institute of Certified Public Accountants), 2001, June 15

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

The CPA. Never Underestimate The Value℠

Chartered Accountants of Canada

Comptables agréés du Canada

EXPOSURE DRAFT

AICPA/CICA

WebTrust SM/TM Program

Confidentiality Principle and Criteria

June 15, 2001

Version 3.0

Comments on this exposure draft should be sent to Karyn Waller, Senior Technical Manager, Trust Family Services, AICPA, 1211 Avenue of the Americas, New York, NY 10036-8775 or Bryan Walker, Canadian Institute of Chartered Accountants, 277 Wellington Street West, Toronto, Canada M5V 3H2 in time to be received by July 31, 2001. Responses also may be sent by electronic mail via the Internet to kwaller@aicpa.org or bryan.walker@cica.ca

COMMITTEE AND TASK FORCE MEMBERS

AICPA
Assurance Services Executive Committee

Susan C. Rucker, *Chair*

Gari Fails

Ted Horne

Everett C. Johnson, Jr.

John Lainhart

J. W. Mike Starr

Wendy E. Visconty

Thomas E. Wallace

Neal West

CICA
Assurance Services Development Board

Doug McPhie, *Chair*

Diana Chant

Douglas C. Isaac

Marilyn Kuntz

Jeff Orchard

Frederick J. Phillips

Doug Timmins

Keith S. Vance

AICPA Staff Contacts:

Alan W. Anderson,
Senior Vice President of Member & Public Interests

Anthony J. Pugliese,
Vice President, Member Innovation

J. A. Louis Matherne
Director, Business Assurance and Advisory Services

Karyn Waller
Senior Technical Manager, Trust Family Services

CICA Staff Contacts:

Cairine M. Wilson,
Vice President, Innovation

Gregory P. Shields
Director, Assurance Service Development

Bryan Walker, CICA
Principal, Assurance Services Development

AICPA / CICA Electronic Commerce
Assurance Services Task Force

Everett C. Johnson, Jr., *Chair*

Bruce R. Barrick

Jerry R. DeVault

Joseph G. Griffin

Christopher J. Leach , *Vice Chair*

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Alfred F. Van Ranst

CONTENTS

WEBTRUST CONFIDENTIALITY PRINCIPLE AND CRITERIA

Introduction

In the course of communicating and transacting business over the Internet (or a more focused business Extranet), business partners must send and receive information about the other party that needs to be maintained on a confidential basis. In most instances, parties who are interested in engaging in electronic commerce (e-commerce) will be anxious to ensure that the information they provide is available only to those individuals who need access to complete the transaction or follow-up on any questions that arise.

To enhance business partner confidence in e-commerce, it is important that the business partner is informed about the entity's confidentiality practices for e-commerce transactions. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to, uses and shares information designated as confidential.

Unlike personally identifiable information (i.e., private information), which is being defined by regulation in a number of countries worldwide, there is no widely recognized definition of confidential information. Also, unlike personal private information, there are no defined rights of access to confidential information to ensure its accuracy and completeness. As a result, interpretations of what is deemed to be confidential information can vary significantly from business to business and in most cases is driven by contractual arrangements. As a result, it is important for those engaged, or expecting to be engaged, in business relationships to understand and to accept what information is to be maintained on a confidential basis and what, if any, rights of access or other expectations that an entity might have to update that information to ensure its accuracy and completeness.

Information that is provided to another party is susceptible to unauthorized access during transmission over the Internet and while it is stored on the other party's computer systems. For example, business partner profile information, transaction and settlement instructions may be intercepted by an unauthorized party while they are being transmitted over the Internet. However, if the information is encrypted, it is difficult for the unauthorized party to decipher it. Also, if the computer system where the data is stored is not protected by a firewall and a rigorous system of access controls, unauthorized persons may access the information.

WebTrust Confidentiality focuses on confidential information obtained as a result of e-commerce from existing or potential business partners. The WebTrust Confidentiality Principle sets out an overall objective for the confidentiality of data exchanged over electronic networks such as the Internet or a Virtual Private Network. The privacy of personally identifiable information is covered in WebTrust Program for Online Privacy. In the course of a WebTrust examination, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

Scope of Work

WebTrust Confidentiality focuses on information designated as confidential and obtained online from business partners as a prelude to or as a result of e-commerce. Where such information is commingled with information obtained by other means, however, the practitioner will need to consider the entity's confidentiality practices and related controls covering all such information.

Examples of information subject to confidentiality include:

- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists

Examples of personally identifiable information subject to privacy include:

- Name, address and home phone number
- Banking information about individuals
- Health information
- Employee earnings
- Individual credit history

The WebTrust Confidentiality Principle

> *The entity discloses its confidentiality practices, complies with such confidentiality practices, and maintains effective controls to provide reasonable assurance that access to information obtained as a result of electronic commerce and designated as confidential is restricted to authorized individuals, groups of individuals, or entities in conformity with its disclosed confidentiality practices.*

To enhance business partner confidence in e-commerce, it is important that the business partner is informed about the entity's confidentiality practices for e-commerce transactions. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to, uses and shares information designated as confidential.

The WebTrust Criteria[1]

The WebTrust Criteria are organized into four broad areas – disclosures, policies, procedures and monitoring.

A three-column format has been used to present and discuss the criteria. The first column presents the criteria—the attributes that the entity must meet to be able to demonstrate that it has achieved the principle. The second and third columns provide illustrative disclosures and controls for business-to-business transactions and for transactions applicable to service providers. These are examples of disclosures the entity might make and controls that the entity might have in place to comply with the criteria. Alternative and additional disclosures and controls also can be utilized to comply with the criteria.

For the purpose of these criteria, the term "business partner" also includes individuals who may provide confidential information (as opposed to personally identifiable information).

[1] These criteria meet the definition of "criteria established by a recognized body" described in the third General Standard for attestation engagements in the United States (AICPA, *Professional Standards,* vol. 1, AT sec. 101.25 and in the standards for assurance engagements in Canada (CICA *Handbook,* paragraph 5025.41).

WebTrust Principle and Criteria
Confidentiality

Principle

The entity discloses its confidentiality practices, complies with such confidentiality practices, and maintains effective controls to provide reasonable assurance that access to information obtained as a result of electronic commerce and designated as confidential is restricted to authorized individuals, group of individuals, or entities in conformity with its disclosed confidentiality practices.

Criteria	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
A **Disclosures**		
A.1 The entity discloses its confidentiality practices on its Web site, or through alternative means, before the confidential information is provided. These practices include, but are not limited to, the following disclosures: • How information is designated as confidential and ceases to be confidential. • How access to confidential information is authorized. • How confidential information is used. • How confidential information is shared. • If information is provided to third parties, disclosures should include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity. • If such a process exists,	XYZ-manufacturing.com is a high quality custom manufacturer of electronic components. Customers and potential customers can submit engineering drawings, specifications and requests for manufacturing price quotes through our Web site or electronic mail. Access to your information is limited to our employees and any third-party sub-contractors we may elect to use in preparing our quote. We will not use any information you provide for any purpose other than a price quote and subsequent manufacturing and order fulfillment on your behalf. However, access may need to be provided in response to subpoenas, court orders, legal process or other needs to comply with applicable laws and regulations. Using our encryption software, you may designate information as "confidential" by checking the Confidential Treatment Box. This software can be	B2Bexchange.com is a business-to-business transactional marketplace. Although many features of B2Bexchange.com are available to anonymous companies, companies who wish to take full advantage of B2Bexchange.com must register, and then be authorized by B2Bexchange.com, prior to making transactions. By registering, companies take advantage of various customized features. During registration, companies must supply information required to enable transactions, including, but not limited to user ID, password, ship-to address, contact email address, and country. Contact information from the registration form is used to facilitate the company's ability to transact business on the site, and to contact the company when necessary. We do not resell confidential information to other companies. Demographic and profile data is collected at our site. B2Bexchange.com uses this information to tailor our service to suit the needs of our customers. We do not share information about companies with any third party except as described in this Confidentiality Policy and the

Criteria	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
the entity's alternative dispute resolution process. • Any confidentiality practices needed to comply with applicable laws and regulations.	downloaded from our site and will accept information in most formats. Such information will automatically be encrypted using our public key before transmission over the Internet. You may transmit such information to us through our web site or by e-mail. Access to information designated as "confidential" will be restricted only to our employees with a need to know. We will not provide such information to third parties without your prior permission. When we provide information to third parties, we do not provide your company name. However, we make no representation regarding their confidential treatment of such information. Our confidentiality protection is for a period of two years, after which we will cease to provide such protection. In addition, should such information become public through your actions or other means, our confidentiality protection ceases. If you are not a customer at the time of submitting such information, you will be provided with an account number and password. You may use this account number and password to access the information you have	Membership Agreement. **Supplementation of Information** This site supplements the information that you provide with information that is received from third parties. For instance, verification of information provided during the registration process is required before the company's account is activated. **Use of Aggregated Information** We will not sell or rent confidential information to anyone. Aggregated information is that which describes the collective habits and other common traits of all our members as a group, and which never identifies a particular company. We may send confidential information about you to other companies or people when: • We have your consent to share the information; • We need to share your information to provide the product or service you have requested or to consummate the transaction for the sale or purchase of products by you through the Exchange once a bid has been accepted, forming the basis for an agreement between a Buyer and a Seller (as such terms are defined in the Membership Agreement); • We need to send the information to companies who work on behalf of B2Bexchange.com to

Criteria	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
	submitted, plus any related price quote information provided by us. You may also set up an additional 10 sub accounts and passwords so that others in your organization can also access this information. Our services and the protection of confidential information are subject to third-party dispute resolution. This process is described under "Arbitration Process" [hotlink] elsewhere on our web site.	provide a product or service to you. (Unless we tell you differently, these companies do not have any right to use the information we provide to them beyond what is necessary to assist us.); • We respond to subpoenas, court orders or legal process or otherwise need to comply with applicable law. **External Links** This Web site contains links to other sites. Please be aware that we are not responsible for the confidentiality practices of such other sites. We encourage our companies to be aware when they leave our site and to read the confidentiality statements of each and every web site. This Confidentiality Policy applies solely to information collected by this Web site and service. **Security of Information** At B2Bexchange.com, we appreciate your concerns about the security of your confidential online business transactions. B2Bexchange.com takes security measures to protect any information passed between our site and your computer during transactional sessions. We use Secure Socket Layers to encrypt the information you send us during a session. From the moment you enter the members only area of B2Bexchange.com to the moment you leave, all data transferred between your browser and our servers is encrypted. This ensures that everything from your user

Criteria	Illustrative Disclosures for Business-to-Business E-Commerce	Illustrative Disclosures for Service Providers
		name and password to your internal document numbers and order details are never passed across the Internet "in the clear". You may edit your account information at any time by visiting the following web address: www.B2Bexchange.com/members/admin
A.2	The entity discloses how to contact it for questions or support and how to inform it about breaches or possible breaches to the confidentiality of information and security of its related systems.	If you have any questions about our organization or our policies on confidentiality as stated at this site, please contact CustServ@XYZ-manufacturing.com. Should you feel that there has been a breach to the security of this site please contact us *immediately* at (800) 123-1234.
A.3	The entity discloses changes or updates to its confidentiality practices.	Effective January 2001 we eliminated our "secret" category of information. Information submitted under such secret category will continue to be protected accordance with our commitments at that time.

Criteria	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
B	**Policies[2]**	
B.1	The entity's policies related to the protection of confidential information include, but are not limited to, the following items[3]: • Who is allowed access, what is the nature of that access, and who authorizes such access. • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access • Complaint resolution process. • Procedures to handle security incidents. • Controls over physical access to the system(s). • Security procedures to protect confidential information.	The company's policy provides detailed guidelines for user profile creation, modification and deletion along with the assignment of corresponding permissions for the user. Management has in place a hotline to allow business partners to communicate any comments, complaints, or concerns regarding the confidential treatment of information and security of the site. The Company has a policy of using arbitration not satisfactorily addressed through the complaint procedures. Policies provide for employees and business partners to report a breech or suspected breech of the confidentiality and related security of the Web site. Employees are required to report such incidents within two hours of the breech (or suspected breech). Business partners are encouraged to call the toll-free number posted at the company Web site. Physical access is controlled through a combination of guarded entrances, card key access, and monitoring cameras. Our company's defined security policy details access privileges, information collection needs, accountability, and other such matters. It is reviewed and updated at quarterly management meetings and undergoes an intense review on an annual basis by the Information Technology (IT) department. Documented system security objectives, policies, and standards are consistent with system security requirements defined in contractual, legal, and other service level agreements. For example, current policy prohibits shared IDs; each support person has his or her own unique ID to log on and maintain network equipment. A complete policy with details regarding access, scripting, updates, and remote access are available for review by qualified personnel. This document is not available to the general public. Access to the business partner's confidential information for update and corrective purposes is provided through use of its unique ID and password. Proper historic audit trails of business partner communications

[2] Policies are rules that provide a formal direction for achieving business and performance objectives and that enable enforcement. Standards are required procedures that are implemented to meet the policies. In some entities, policies and standards represent separate items; in other entities, they are terms that are used interchangeably.

[3] Often an entity's confidentiality policy is addressed within the broader context as part of its information or data security policy statement.

Criteria	Illustrative Controls for Business-to-Business E-Commerce	Illustrative Controls for Service Providers
	are maintained for any needed follow-up. These records are maintained for the time mandated by the cognizant regulatory agency or legal entity, after which time they are deleted. The record retention and deletion policy is reviewed on a periodic basis by company management.	
B.2 The employees responsible for information security and related confidentiality of information are aware of and follow the entity's security and related confidentiality policies.	As part of their orientation, the confidentiality and related security policies are reviewed with new employees and the key elements of the policies and their impact on the employee are discussed. The employee must then sign a statement signifying that they have read, understand, and will follow these policies. Each year, as part of their performance review, employees must reconfirm their understanding of and compliance with these policies. Employees who deal with confidential information are required to undergo an annual training and awareness program.	
B.3 Accountability for management of the entity's policies related to confidentiality and relevant security matters has been assigned.	Management has assigned responsibility for enforcement of the company confidentiality and security policies to the chief information officer (CIO). Others on the executive committee assist in the review and update of the policies as outlined in the executive committee handbook.	
B.4 The entity has allocated resources for awareness and support of its policies related to confidentiality and relevant security matters.	The company has budgeted for confidentiality and security training. This amount is reviewed quarterly to ascertain whether additional training is needed based on employee feed back as well as changes in confidentiality and security policies and procedures.	Management has an on-going confidentiality and security training program for all employees. IT staff is required to submit an annual training request based on job description. All employees are given periodic confidentiality and security training courses put on by the IT Department. The CIO evaluates these programs and makes a quarterly report to the executive committee.

Criteria	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers

Procedures

Security Criteria That Relate to Confidentiality

C.1	The entity has security procedures to establish new users.	The business partner's designated administrative user uses a secure session to authorize new users and select an appropriate user identification (ID) and password and level of access for each of its users.	
C.2	The entity has security procedures to identify and authenticate authorized users.	All external users are required to provide a unique user ID and password to place an order or access their specific business partner information. System level access to all production systems (for example, UNIX and Windows NT) is provided via a strong identification and authentication mechanism (digital signature, one-time password, SecureID, or other system). Strong, static passwords are used for systems that do not require a strong identification and authentication mechanism. Controlled access by a software authentication product with a strong identification and authentication mechanism is required for access to any routers.	
C.3	The entity has procedures to allow users to change, update, or delete their own user profile.	In order to update, change, or delete user information, the user's current ID and password are required. After providing this information in a secure session, the user can proceed to the user profile section for any changes.	All changes to user profiles are done after providing user ID and password. The only changes allowed are updates to the user ID and password. Changes to personal information or deletions must be processed in writing.
C.4	The entity has procedures to limit remote access to the internal network to only authorized entity personnel.	Logical access control procedures (for example, firewalls, routers, and password controls) are maintained by the information technology (IT) department. These controls are tested on a periodic basis by performing penetration testing from both within the internal network and from the Internet. Remote access is provided to key employees; the system accepts remote calls, verifies the user, and then hangs up and	The remote access to and use of the computing resources are restricted by the implementation of an authentication mechanism for identified users and resources associated with access rules.

	Criteria	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
		calls the user back at the authorized number. Identification and authorization is accomplished through the combination of user ID and one-time password.	User IDs and passwords are stored in an encrypted database, with the associated encryption key stored off-line.
C.5	The entity has procedures to prevent business partners, groups of individuals, or other entities from accessing information other than that which they are authorized to access.	Business partners are required to enter a user ID and password to access the confidential information that they are authorized to access.	One-time passwords and/or smart cards restrict all system access from outside the entity, other than for customary e-commerce transactions through the Web page. Business partner Web sites hosted by the Internet Service Provider (ISP) are prevented from intercepting messages not addressed to them. Packet filters are implemented on the ISP Internet gateway routers using access control lists (ACLs) according to the ISP firewall policy. Anti-spoof filters are used on the routers to prevent spoofing of trusted sources. Additional ACLs are used to control business partner access to only their network segments. The various LAN segments are firewalled from the rest of the networks.
		The use of strong authentication and authorization procedures are in place. The authentication process allows the user to access only information relevant to that particular user. Other methods are in place to detect users attempting to guess another password or if a brute force attack is under way. If such an attack is detected, the system will disconnect from the user and report the security breach for follow up.	
C.6	The entity has procedures to limit access to confidential information to only its authorized employees based upon their assigned roles and responsibilities consistent with its disclosed	Employee access to business partner data is limited to individuals based upon their assigned responsibilities. Idle workstations are timed-out after thirty minutes. Access to the corporate information technology facilities is limited to authorized employees by use of a card/key system supported by video surveillance monitoring.	

	Criteria	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
	confidentiality practices.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to confidential information based on job function and need. Other business partners are subject to non-disclosure agreements (NDAs).	
C.6.1	The entity secures its programs and data during the backup, off-site storage, and restoration processes.	During the daily backup routine, the data is secured from both physical and logical access by unauthorized personnel. During any restoration process, no access is allowed by unauthorized personnel.	
C.7	The entity utilizes a minimum of 128-bit encryption to protect transmission of user authentication, verification, and confidential information that is passed over the Internet from unintended recipients.	Confidential information is protected during transmission by using 128-bit encryption technology (SSL technology). The company's Web site has a digital certificate that can be checked using features in a standard Web browser.	
C.8	The entity has procedures to maintain system configurations that minimize security exposures that potentially affecting confidential information.	Company management routinely evaluates the level of performance it receives from the ISP that hosts the company Web site. This evaluation is done by evaluating the security controls the ISP has in place by an independent third party as well as by following up with the ISP management on any open items or causes for concern.	The service provider meets with its technology vendors on a regular basis (for example, SUN, Cisco and Microsoft). Identified vendor security issues are documented and conveyed to the vendor to the appropriate level of management, depending on the severity of the exposure and risks associated with its planned or current deployment in the network. All vendor security issues are associated with agreed upon time frames and followed up on by an ISP representative.
C.9	The entity has procedures to monitor and act upon confidentiality and security breaches.	System logs are monitored and evaluated on a daily basis. Monitoring software is in place that will notify the IT manager via e-mail and pager should any incident be in progress. If an incident occurs, a report is filed within twenty-four hours for follow-up and analysis.	

Criteria	Illustrative Controls for Business to Business E-commerce	Illustrative Controls for Service Providers
	Business partners are directed to an area of the Web site to post a message about breaches or suspected breaches as soon as they become concerned. These business partner comments are followed up within twenty-four hours for evaluation and a report is issued back to the business partner and CIO or the business partner may contact the Incident Response hot-line by telephoning (888) 911-0911 24x7.	
Confidentiality Specific Criteria		
C.10 The entity has procedures to ensure that confidential information obtained as a result of electronic commerce is only disclosed to parties consistent with its disclosed confidentiality practices.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has access to other individuals or entities. Appropriate access controls are in place that limit access to confidential information based on job function and need. Other business partners are subject to non-disclosure agreements (NDAs).	
C.11 The entity has procedures to obtain assurance or a representation that the adequacy of confidentiality policies of third parties to whom information is transferred, and upon which the entity relies, is in conformity with the entity's disclosed confidentiality practices.	The entity outsources technology support or service and transfers data to the outsource provider. The entity obtains representation as to the controls that are followed by the outsource provider and obtains a report on the effectiveness of such controls from the outsource provider's independent auditor.	
C.12 In the event that a disclosed confidentiality practice is deleted or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the confidentiality practices in place when such information was received, unless the business partner agrees to the change in practice.	The entity maintains copies of all versions of the confidentiality policy. The entity attorney summarizes the key changes to this policy statement. When changes to a less restrictive policy are made, the company attempts to obtain the agreement of its customers to the new policy. Confidential information for those customers who do not agree to the new policy is isolated and receives continued protection under the old policy.	

Criteria	Illustrative Controls for Business-to-Business E-commerce	Illustrative Controls for Service Providers
D Monitoring		
D.1 The entity has procedures to monitor the security of its electronic commerce systems and to identify any need for changes to its confidentiality and related security controls.	The Information Security group uses the following monitoring tools: • COPS – This software provides a snap shot of the system, which is analyzed on a monthly basis. • Tripwire – This is a real time monitor, which is used to detect intruders. • SATAN – This software is run monthly and provides a security analysis of the system. In addition, the group maintains and analyzes the server logs.	Commercial and other monitoring software (for example, COPS, SATAN and ISS) is run on a routine basis. The report output from these programs is analyzed for potential weaknesses and threats to the systems. Changes are made due to the information contained in these reports and with the consultation and approval of management.
D.2 The entity has procedures to monitor environmental and technology changes, and the related risks, to keep its disclosed confidentiality practices and related policies consistent and current with laws and regulations.	Management reviews its disclosed confidentiality policies maintained at the Web site on a quarterly basis and evaluates its compliance to these policies. Management makes any changes or needed modifications to the policy or disclosure within five business days of its evaluation. Laws and regulations that affect the disclosed site confidentiality policy are evaluated and reported on by the corporate attorney at least annually or when new regulations require an update. Staff meetings are held on a regular basis to address current privacy concerns and their findings are discussed at quarterly management meetings. The company subscribes to publications and user groups specific to its industry and application in order to receive the most current security information. On a monthly basis the Webmaster reports to the CIO any weaknesses perceived in the system. Management reviews this report for follow-up and resolution.	

	Criteria	Illustrative Controls for Business-to-Business E-commerce	Illustrative Controls for Service Providers
D.3	The entity has procedures in place to monitor its security incident procedures and update these as needed due to technology changes, changes in the structure of the electronic commerce system(s), or other information.	Weekly IT staff meetings are held to address current security concerns and the findings are discussed at quarterly management meetings.	Senior management reviews the security policy on a biannual basis and considers developments in technology and the impact of any laws or regulations.
D.4	The entity has procedures to monitor noncompliance with confidentiality and relevant security disclosures and corrective action is taken on a regular and timely basis.	Security issues are recorded and accumulated in a problem report. Corrective action is noted and monitored by management.	