Security Disclosures for Ariba Online Services

Ariba is committed to the security and integrity of customer information within Ariba Online Services. Ariba uses industry best-practice security measures to protect against the loss, misuse or alteration of the information under our control.

To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect within the Ariba Online Services*. These measures include the following:

- Multiple level firewalls to segregate and secure network segments based on system roles.
- Data transmissions are encrypted using SSL technology
- Use of server-side and client-side digital certificates
- Role-based administrative access policies and procedures
- Primary co-location facility uses cipher-encoded access badges, biometric scans, and 24-hour video surveillance and guards to control access
- Comprehensive in-house performance and security monitoring and auditing
- Intrusion detection and analysis
- Detailed security policy, processes and procedures
- Security auditing performed by outside consulting agencies

To provide for the availability of service and information within Ariba Online Services, Ariba implements the following components:

- A disaster recovery plan
- Detailed backup strategy and secure off-site storage
- High availability clustered database servers
- Redundant systems, power supplies, and network connections
- Service level agreements with service providers to guarantee service levels
- Comprehensive change management and testing policies
- 24-hour x 7-day per week support staff for Severity Level 1 issues.

The Ariba Technical Overview document for the specific Ariba Online Services you are using contains detailed information concerning policies, procedures and architecture. This document is available by request to customers pursuant to a separate non-disclosure agreement.

If you have any concerns regarding any of the above information please contact Ariba Customer Support Services.

*These Security Disclosures do not apply to the following Ariba Online Services: Ariba QuickSource 6.1. The Ariba Network has Network-specific Security Disclosures listed online at http://www.ariba.com/webtrust.cfm.

Note: The English version of these Security Disclosures shall govern in the event of any conflict or substantive translation changes into a non-English language.

*****

Last Updated 07 July 2006