

Compliance: Sarbanes-Oxley

How a Secure File Transfer Solution Should Support Compliance

Confidentiality	Sarbanes-Oxley – CoBIT	How WS_FTP Server and WS_FTP Professional Support Compliance
Authentication	DS5.3 Identity Management. All users and their activity should be uniquely identifiable.	<ul style="list-style-type: none"> - Unique user IDs - Integrates with existing user databases such as Active Directory, LDAP, NT and ODBC databases - Active Directory support for Distinguished Name, Group and Organizational Unit - All passwords encrypted during client-server authentication when using WS_FTP Professional and WS_FTP Server - All passwords stored in WS_FTP Server database are encrypted - Ability to enforce strong password creation - Auto-expiring passwords with options to allow client reset - Rules on using previously used passwords - Two-factor authentication using username/passwords pairs, with SSL Certificates for mutual authentication, or with SSH public keys
Access Control	<p>DS5.3 Identity Management. User identities and access rights are maintained in a central repository.</p> <p>User access rights to systems and data should be in line with defined and documented business needs and job requirements.</p> <p>Technical measures are deployed to establish user identification, implement authentication and enforce access rights.</p>	<ul style="list-style-type: none"> - Administrative SoD (Separation of Duties) with multiple levels of access control and administrator permissions - Permissions can be set on shared folders and applied to individual users or entire user groups - Administrators can set disk space, maximum file storage, and maximum bandwidth for entire groups or users - Block file uploads, downloads, deletions, renaming, and directory creation on a per user basis and per IP address - Set read, write, delete, list, and rename permissions on shared folders - Lock users to their home folder, hide other folders from view - Administrative options to hide the existence of other users' folders - Control server access by IP address and port ranges - Block IP addresses manually, or automatically, using set criteria (such as number of failed connections), - Block IP addresses by subnet - Support for IP address "whitelist" (safe from automatic blocking) - Virtual folders are supported for accessing Universal Naming Convention (UNC) and mapped drives - Create SSL certificates and a trusted authorities database on a per host basis - Force mutual authentication for client and server to both exchange SSL certificates - Clear Command Channel (CCC) enables Firewall/Network Address Translations (NAT) support for SSL connections - Configure IP address and ports when using PASV command (with or without SSL) for better performance with firewalls, NAT devices - User IDs and passwords always encrypted
Privacy	DS5.11 Exchange of Sensitive Data. Exchange only over a trusted path, control for content authenticity, proof of submission, proof of receipt and non-repudiation of origin.	<ul style="list-style-type: none"> - Encrypts client connections over SSH, SSL (Version 3—Implicit, Explicit and TLS) and SCP2 protocols - Session encryption using 256-bit AES encryption and 3DES - FIPS 140-2 validated encryption using 256-bit AES, 3DES, and SHA 1, SHA 2 - Force SSH, SSL/FTPS or TLS 1.0 or higher on all client connections to WS_FTP Server 128 bit SSL on folder access - Encrypts stored files with fully-integrated OpenPGP mode - Configurable SSL/TLS encryption down to the folder level - Policy based cryptographic strength enforcement - Import, export and create SSL x.509v3 certificates - Support for full chain and peer-level SSL certificate chains - Import, export and create SSH keys, including OpenSSH keys, for Windows, Unix, and Linux - Support for suppressing SSH protocol name in version in login banner, preventing malicious actions - Create, Edit, Import, Export, Delete OpenPGP keys with support for PGP, OpenPGP and GPG - Select and prioritize ciphers to use in OpenPGP key creation - Support for RSA and Diffie-Hellman key types with settable expiration date - OpenPGP asymmetric key length of 1024 – 4096 bits

Compliance: Sarbanes-Oxley

How a Secure File Transfer Solution Should Support Compliance

Visit www.ipswitchFT.com to learn more about Ipswitch Secure File Transfer solutions.

Integrity	Sarbanes-Oxley – CoBIT	How WS_FTP Server and WS_FTP Professional Support Compliance
	<p>PO2.4 Integrity Management. Define and implement procedures to ensure integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.</p>	<ul style="list-style-type: none"> - Built-in file integrity checking of up to SHA-512 secure hashing algorithms - Encrypts stored files with fully-integrated OpenPGP mode - Encrypts client connections over SSH and SSL (Implicit, Explicit and TLS) protocols - Session encryption using 256-bit AES encryption and 3DES - File and folder size comparing to ensure accuracy and completeness - Syslog integration into centralized network or security management logging systems - Automate the mirroring of two locations with built-in schedule, synchronization and backup utilities - File lock during upload prevents users from downloading a file before it is fully uploaded to the server - FIPS 140-2 validated ciphers using WS_FTP FIPS-validated transfer mode
Availability	<p>AI2.4 Application Security and Availability. Address application security and availability.</p> <p>AI3.2 Infrastructure Resource Protection and Availability. Implement controls to protect resources and ensure availability.</p> <p>DS1.5 Monitoring and Reporting of Service Level Achievements. Continuously monitor specified service level performance criteria.</p> <p>DS3.5 Monitoring and Reporting. Continuously monitor the performance and capacity of IT resources.</p> <p>DS4.3 Critical IT Resources. Focus attention on critical items, build in resilience recovery priorities.</p> <p>DS11.1 Business Requirements for Data Management. Ensure that source documents expected from the business are received, processed, output prepared and delivered, and restart and reprocessing needs are supported.</p> <p>DS11.6 Security Requirements for Data Management. Establish arrangements to identify and apply security requirements applicable to the receipt, processing, physical storage and output of data and sensitive messages. This includes physical records, data transmissions and any data stored offsite.</p>	<ul style="list-style-type: none"> - Server architecture enables load balancing to distribute workload among multiple servers for improved performance - Clustering groups servers for redundancy and to overcome scheduled/unscheduled server downtime - Session manager delivers real-time performance statistics on WS_FTP Server connections and file transfer events - Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files - Administration Logging: Keep an auditable record of server administrator actions - Syslog Support: Integrate WS_FTP logs with a company database or central data repository - Logging server and notification server both require administrator login - Ability to install logging server and notification server on a different server to optimize availability - Automatic restart of interrupted file transfers so users never lose valuable data because of an interrupted connections - Multipart mode splits large files into smaller segments and downloads all segments via different, yet concurrent, connections - File compression enables faster file transfers by reducing the size of files - Scheduler lets you program one-time or recurring transfers with auto-login, navigation and transfer - Backup wizard automates file backup to any device, drive or FTP server - Synchronize files and file directories between any two locations - Automated notifications trigger communication, workflows. Email, SMS and pager alerts. Launch external programs on events. - Configure to execute an application and include command line variables - Firewall script engine enables script creation. Firewall Wizard steps through multiple firewall types including HTTP Proxy - Prevents DOS attacks by blocking IP addresses manually, automatically, using criteria such as number of failed connections.
Audit	<p>DS13.3 IT Infrastructure Monitoring. Define and implement procedures to monitor the IT infrastructure and related events. Ensure sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.</p> <p>DS5.5 Ensure that IT security implementation is monitored proactively. Access to the logging information is in line with business requirements in terms of access rights and retention requirements.</p> <p>ME3.5 Integrated Reporting. Integrate IT reporting on regulatory requirements with similar output from other business functions.</p>	<ul style="list-style-type: none"> - Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files - Administration Logging: Keep an auditable record of server administrator actions - Syslog Support: Integrate WS_FTP logs with a company database or central data repository - Log viewer provides four levels of reporting including verbose for all client-server activity, administration activity and errors - Nested filtering provides custom views of file transfer or other server events - Logs are exportable in XML format - Automated notifications triggers communication and workflows. Generate email, SMS and pager alerts and launch external programs based on server events such as uploading a file or creating a directory - Log the details of encrypted connections to verify encryption strength and type negotiated for a given session - Session manager delivers real-time performance statistics on WS_FTP Server connections and file transfer events - Connection log shows all commands sent from WS_FTP Professional to a server and shows the replies from the server