

Confidentiality	BASEL II – FFIEC Security Guidelines	How WS_FTP Server and WS_FTP Professional Support Compliance
Authentication	<ul style="list-style-type: none"> - Enforce use of unique user IDs matched to individual users - Select authentication mechanisms based on the risk associated with the particular application or service. - Multifactor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities. - Encrypt the transmission and storage of authenticators whether on public networks or on the financial institution’s network. 	<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	<ul style="list-style-type: none"> - User enrollment process to Add, Delete, Modify user access - Assign users and devices only the access required to perform their required functions, - Provide file, directory and application level access control - Ease the administrative burden of managing access rights by utilizing software that supports group profiles. 	<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	<ul style="list-style-type: none"> - Encrypt sensitive information when passing over a public network and also may be encrypted within the institution network. - Use strong authentication and encryption to secure communications. - Use encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk. - Use encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device. - Use trusted public algorithms such as AES, DES and Triple DES, SHA-1, and RSA. 	<ul style="list-style-type: none"> - Encrypts client connections over SSH, SSL (Version 3—Implicit, Explicit and TLS) and SCP2protocols - 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

Integrity	BASEL II – FFIEC Security Guidelines	How WS_FTP Server and WS_FTP Professional Support Compliance
	<ul style="list-style-type: none"> - Use integrity checking software to prevent potential malicious activity. - Use encryption to allow discovery of unauthorized changes to data. - Creating cryptographic hashes of key files. 	<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		
	<ul style="list-style-type: none"> - Determine whether appropriate access controls and physical controls have been considered and planned for the replicated production system and networks when processing is transferred to a substitute facility. - Determine whether the security monitoring and intrusion response plan considers the resource availability and facility and systems changes that may exist when substitute facilities are placed in use. 	<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 firewall 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		
	<ul style="list-style-type: none"> - Log user or program access to sensitive system resources including files, programs, and processes. - Log and monitor the date, time, user, user location, duration, and purpose for all remote access. - Filter logs for potential security events and provide adequate reporting and alerting capabilities. - Log access and security events. - Use software that enables rapid analysis of user activities. - Encrypt log files that contain sensitive data or that are transmitting over the network. - Ability to send logging data to a separate, isolated computer. 	<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