

Confidentiality	BASEL II – FFIEC Security Guidelines	How WS_FTP Server and WS_FTP Professional Support Compliance
<b>Authentication</b>	<ul style="list-style-type: none"> <li>- Enforce use of unique user IDs matched to individual users</li> <li>- Select authentication mechanisms based on the risk associated with the particular application or service.</li> <li>- Multifactor authentication is increasingly necessary for many forms of electronic banking and electronic payment activities.</li> <li>- Encrypt the transmission and storage of authenticators whether on public networks or on the financial institution's network.</li> </ul>	<ul style="list-style-type: none"> <li>- Unique user IDs</li> <li>- Integrates with existing user databases such as Active Directory, NT and ODBC databases</li> <li>- Active Directory support for Distinguished Name, Group and Organization Unit</li> <li>- All passwords encrypted during client-server authentication when using WS_FTP Professional and WS_FTP Server</li> <li>- All passwords stored in WS_FTP Server database are encrypted</li> <li>- Ability to enforce strong password creation</li> <li>- Auto-expiring passwords with options to allow client reset</li> <li>- Rules on using previously used passwords</li> </ul>
<b>Access Control</b>	<ul style="list-style-type: none"> <li>- User enrollment process to Add, Delete, Modify user access</li> <li>- Assign users and devices only the access required to perform their required functions,</li> <li>- Provide file, directory and application level access control</li> <li>- Ease the administrative burden of managing access rights by utilizing software that supports group profiles.</li> </ul>	<ul style="list-style-type: none"> <li>- Administrative SoD (Separation of Duties) with multiple levels of access control and administrator privileges</li> <li>- Permissions can be set on shared folders and applied to individual users or entire user groups</li> <li>- Administrators can set disk space, maximum file storage, and maximum bandwidth for entire groups or users</li> <li>- Block file uploads, downloads, deletions, renaming, and directory creation on a per user basis and per IP address</li> <li>- Set read, write, delete, list, and rename permissions on shared folders</li> <li>- Lock users to their home folder</li> <li>- Administrative options to hide the existence of other users' folders</li> <li>- Control server access by IP address and port ranges</li> <li>- Virtual folders are supported for accessing Universal Naming Convention (UNC) and mapped drives</li> <li>- Create SSL certificates and a trusted authorities database on a per host basis</li> <li>- Force mutual authentication for client and server to both exchange SSL certificates</li> <li>- Clear Command Channel (CCC) enables Firewall/Network Address Translations (NAT) support for SSL connections</li> <li>- Configure IP address and ports when using PASV command (with or without SSL) for better performance with firewalls and NAT devices</li> </ul>
<b>Privacy</b>	<ul style="list-style-type: none"> <li>- Encrypt sensitive information when passing over a public network and also may be encrypted within the institution network.</li> <li>- Use strong authentication and encryption to secure communications.</li> <li>- Use encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk.</li> <li>- Use encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device.</li> <li>- Use trusted public algorithms such as AES, DES and Triple DES, SHA-1, and RSA.</li> </ul>	<ul style="list-style-type: none"> <li>- User IDs and passwords always encrypted</li> <li>- Encrypts client connections over SSH and SSL (Implicit, Explicit and TLS) protocols</li> <li>- Session encryption using 256-bit AES encryption and 3DES</li> <li>- Force SSH, SSL/FTPS or TLS 1.0 or higher on all client connections to WS_FTP Server</li> <li>- Encrypts stored files with fully-integrated OpenPGP mode</li> <li>- Configurable SSL/TLS encryption down to the folder level</li> <li>- Policy based cryptographic strength enforcement</li> <li>- Import, export and create SSL x.509v3 certificates</li> <li>- Import, export and create SSH keys</li> <li>- Create, Edit, Import, Export, Delete OpenPGP keys with support for PGP, OpenPGP and GPG</li> <li>- Select and prioritize ciphers to use in OpenPGP key creation</li> <li>- Support for RSA and Diffie-Hellman key types with settable expiration date</li> <li>- OpenPGP asymmetric key length of 1024 – 4096 bits</li> </ul>

Integrity	BASEL II – FFIEC Security Guidelines	How WS_FTP Server and WS_FTP Professional Support Compliance
	<ul style="list-style-type: none"> <li>- Use integrity checking software to prevent potential malicious activity.</li> <li>- Use encryption to allow discovery of unauthorized changes to data.</li> <li>- Creating cryptographic hashes of key files.</li> </ul>	<ul style="list-style-type: none"> <li>- Built-in file integrity checking of up to SHA-512 secure hashing algorithms</li> <li>- Encrypts stored files with fully-integrated OpenPGP mode</li> <li>- Encrypts client connections over SSH and SSL (Implicit, Explicit and TLS) protocols</li> <li>- Session encryption using 256-bit AES encryption and 3DES</li> <li>- File and folder size comparing to ensure accuracy and completeness</li> <li>- Syslog integration into centralized network or security management logging systems</li> <li>- Automate the mirroring of two locations with built-in schedule, synchronization and backup utilities</li> <li>- File lock during upload prevents users from downloading a file before it is fully uploaded to the server</li> </ul>
Availability	<ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul>	<ul style="list-style-type: none"> <li>- Server architecture enables load balancing to distribute workload among multiple servers for improved performance</li> <li>- Clustering groups servers for redundancy and to overcome scheduled/unscheduled server downtime</li> <li>- Session manager delivers real-time performance statistics on WS_FTP Server connections and file transfer events</li> <li>- Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files</li> <li>- Administration Logging: Keep an auditable record of server administrator actions</li> <li>- Syslog Support: Integrate WS_FTP logs with a company database or central data repository</li> <li>- Logging server and notification server both require administrator login</li> <li>- Ability to install logging server and notification server on a different server to optimize availability</li> <li>- Automatic restart of interrupted file transfers so users never lose valuable data because of an interrupted connections</li> <li>- Multipart mode splits large files into smaller segments and downloads all segments via different, yet concurrent, connections</li> <li>- File compression enables faster file transfers by reducing the size of files</li> <li>- Scheduler lets you program one-time or recurring transfers with auto-login, navigation and transfer</li> <li>- Backup wizard automates file backup to any device, drive or FTP server</li> <li>- Synchronize files and file directories between any two locations</li> <li>- 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</li> <li>- Configure to execute an application and include command line variables</li> <li>- Firewall scripting engine lets you create and edit firewall scripts and Firewall Wizard walks you through creation of multiple firewall types including HTTP Proxy</li> </ul>
Audit	<ul style="list-style-type: none"> <li>- Log user or program access to sensitive system resources including files, programs, and processes.</li> <li>- Log and monitor the date, time, user, user location, duration, and purpose for all remote access.</li> <li>- Filter logs for potential security events and provide adequate reporting and alerting capabilities.</li> <li>- Log access and security events.</li> <li>- Use software that enables rapid analysis of user activities.</li> <li>- Encrypt log files that contain sensitive data or that are transmitting over the network.</li> <li>- Ability to send logging data to a separate, isolated computer.</li> </ul>	<ul style="list-style-type: none"> <li>- Client-Server Logging: Capture Client-Server connections and activities related to the storage and transfer of files</li> <li>- Administration Logging: Keep an auditable record of server administrator actions</li> <li>- Syslog Support: Integrate WS_FTP logs with a company database or central data repository</li> <li>- Log viewer provides four levels of reporting including verbose for all client-server activity, administration activity and errors</li> <li>- Nested filtering provides custom views of file transfer or other server events</li> <li>- Logs are exportable in XML format</li> <li>- 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</li> <li>- Log the details of encrypted connections to verify encryption strength and type negotiated for a given session</li> <li>- Session manager delivers real-time performance statistics on WS_FTP Server connections and file transfer events</li> <li>- Connection log shows all commands sent from WS_FTP Professional to a server and shows the replies from the server</li> </ul>