Strategies for achieving compliance with blueButler

The PCI-DSS standards take the form of twelve requirements each addressing a specific aspect of PCI data security. These include information access (passwords), network architecture, data storage (encryption), policy compliance (audit trail), retention, and other critical protective measures. Note that there are no PCI-compliant products – it is the company itself that becomes compliant through adherence to these requirements. The table below describes the requirements and how blueButler can be used for compliance with the standards.

PCI Security Standards guidance	**blueButler functionality**
Install and maintain a firewall to protect cardholder data	The blueButler server is installed at the customer premise behind the corporate firewall. The server is connected to the corporate LAN with restricted access only to authorized workstations.
Do not use vendor-supplied defaults for system passwords	When blueButler is installed at the customer site, blueC technical staff design a security profile with the customer's IT staff that includes setting unique login ids and passwords for accessing the server. The blueButler administrator can configure the number of login/password attempts allowed before a user account is disabled and how often users are required to change their passwords.
Protect stored cardholder data	There are procedures that can be established to ensure blueButler does not record credit card information in the audio files that contain the conversations with callers. These methods include: 1. Have one or more persons designated to handle the credit card transaction portion of the call and "transfer the call" to that person(s). The phone that is used by that person is not recorded (or a secondary "extension key" on the phone is used for those calls and is configured to not be recorded). The normal work flow would be to transfer the call as the final step so it doesn't have to be transferred back to the agent. 2. Have the agent click a button in the blueButler .NET client to pause/resume recording when they are taking the credit card information. blueButler will pause the recording for X seconds (typically this is configured between 20 and 30 seconds by the administrator). The recording automatically resumes after the pause so the agents only have to click once. If the caller needs to provide a second credit card, the agent simply clicks to pause again. On some phone systems, the agent could alternatively press a "button" on their phone that does not invoke any action on the phone but is a signal to blueButler to pause the recording. 3. Have the CRM system send a command to blueButler to pause recording when the agent is ready to enter the credit card information into the CRM system. There are Web Services available in blueButler specifically to allow this type of integration. The CRM can issue a command to blueButler to resume recording after the credit card transaction is completed.

PCI Security Standards guidance	blueButler functionality
	When none of these procedures can be implemented, the credit card information will be contained in the audio file. Note that the credit card information is NOT stored in any data file on the blueButler server. In this case, the credit card information is only stored as part of the audio conversation stored in the call recording file. As such, the credit card information is only available if a user is able to access the audio file and listen to the audio of the conversation. blueButler stores all call recording files in a designated Windows folder that can be configured on a separate hard drive on the blueButler server or a network accessible hard drive. The hard drive that contains this Windows folder can be encrypted using an off-the-shelf encryption application such as TrueCrypt. The hard drive remains inaccessible until the designated person enters the encryption password that makes the drive accessible to the blueButler services that in turn enable authenticated users to access recording files according to their user profile. Users access the audio files only through the blueButler user interface. blueButler requires a login id and password to access the SQL database records associated with the audio files. The user's blueButler profile determines which files the user is allowed to access. NOTE that credit card data is NOT stored in the SQL record associated with the recording. blueButler can synchronize with Microsoft's Active Directory if LAN-based authentication is being used. The blueButler administrator configures how often users must change their passwords if Active Directory synchronization is not utilized.
Encrypt transmission of data across open and public networks	blueButler has three methods available for accessing call recording files. The 1st method is a Java-based web interface. Customers can encrypt this interface by registering the domain that the blueButler server is connected to with SSL encryption. The 2nd method is a .NET client application that resides on the user workstation. The connection between the .NET client and blueButler server utilizes the Microsoft standard .NET framework methodology. If the user is using the .NET client on a public or open network connection to the blueButler server, they would first establish a VPN connection between their PC and the corporate network where the blueButler server resides. The third option is to playback the recording over the phone. This option causes the server to call the user over the telephone network in the same manner that the original caller talked to the user who took the credit card information so it is inherently secure.
Use and regularly update antivirus software	The blueButler server runs either Windows 2003, 2008, Windows 7 or XP Professional. Customers determine what antivirus software to install on the server and how frequently to update it. blueButler is designed to auto-restart the recording services if anti-virus and/or Windows operating system automated updates are enabled to ensure that call recording is not inadvertently disabled by these processes.

PCI Security Standards guidance	**blueButler functionality**
Develop and maintain secure systems and applications	Security is a key part of the architectural design of blueButler. Users are not allowed to directly access recording files; they can only stream the audio if they are authorized to listen to a recording. If the blueButler web service is used by a 3rd-party application to access a recording, blueButler will authenticate the user before the request is granted. The blueButler administrator can further protect the system by disabling the user's ability to download or email a copy of an audio file if required.
Restrict access to cardholder data by business need-to-know	blueButler requires a login id and password to access the SQL database records associated with the audio files. The user's blueButler profile determines which files the user is allowed to access. Typically, a supervisor is permitted access to recordings only for users in their group and managers can access recordings for their departments. If users are given access to recordings it is normally limited to just their own conversations. NOTE that credit card data is NOT stored in the SQL record associated with the recording.
Assign a unique ID to each person with computer access	Each blueButler user is assigned a blueButler User ID that must be unique.
Restrict physical access to cardholder data	The blueButler server is normally installed in a secure computer server room with access restricted to only designated IT staff.
Track and monitor all access to network resources and cardholder data	blueButler maintains log files that contain records on all user interactions with the system including access to individual call recording files. Administrator reports are available to monitor user activity in these log files.
Regularly test security systems and processes	This is a customer responsibility.
Maintain information security for employees and contractors	This is a customer responsibility.