



Welcome to the first Radiant Retail Data Security Bulletin. You can expect to receive these bulletins on the 1st and 3rd Monday of the month. The purpose of these bulletins is to provide you with data security information and best practices. In addition to these bulletins, this data security information will be posted on the [data security section](#) of the Retail Channel Portal, mySARA.

Radiant will also have a monthly Data Security Webinar for you on the 1st Wednesday of the month. The purpose of these webinars is to answer your questions about the information contained in the data security bulletins. Our first webinar will be on Wednesday May 5 at 3:00 PM EST. [Register here](#).

## Security Practice #1 - Implementing Secure Remote Access Processes

Breaking into a system through insecure remote connections is one of the most common tactics criminals use to steal sensitive consumer data. It is extremely important that you are using secure practices when remotely supporting your customers' sites.

While there are many tools available with a wide range of functionality, one requirement applies to all of them. You must make sure you are implementing them in a secure manner. If you are unable to implement a tool according to the guidelines below, it is not suitable for securely supporting your customers. In addition to your support needs, the guidelines below should also be followed by your customers when using tools to access their sites remotely.

### What to do when selecting/configuring a remote access tool:

1. Ensure all default passwords are removed from the remote access software and use unique and complex passwords for each customer.
  - o Passwords should be at least 7 characters long and include both alphabetic and numeric characters
2. Ensure there is a mechanism in place for rotating passwords every ninety days.
3. Ensure encrypted data transmission of at least 128 bits is enabled on the remote access software.
4. Ensure account lockout after a maximum of 6 failed login attempts is enabled.
5. Ensure there is a mechanism for forcing automatic logoff after 30 minutes of inactivity.
6. Ensure the logging function on the remote access software is enabled.

### What NOT to do when selecting/configuring a remote access tool:

- Do not use "free" versions of remote access tools. These versions are for personal use only and are not approved for business use.
- Do not use Windows Remote Desktop without:
  - Running it over a secure protocol such as a Virtual Private Network (VPN) connection through a firewall.
  - Using two-factor authentication to sign in to the Terminal Servers.
  - Using a dedicated SQL Server on a separate logical network.
- Telnet should never be enabled at your customer sites due to significant security concerns.

If you have questions or concerns about implementing these guidelines with your specific remote access tool, your first line of support should be the technical support contact for that tool. If you have additional questions related to remote access best practices, email us at [datasecurity@radiantsystems.com](mailto:datasecurity@radiantsystems.com).

These guidelines help secure your business today. Please note, however, that there are more requirements than outlined here to be PCI compliant. More information about PCI requirements may be

found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).