Passwords:
Simplifying the Rules

Password Creation: Avoid using personal information as this can be researched. Reference song lyrics, a quote you love, or a favorite place.

Password Length: The longer, the better! The minimum requirement should be 10-12 characters.

Password Structure: Strong passwords should also include the use of special characters, a mix of uppercase and lowercase letters, and a mix of both numbers and letters.

Change Passwords Regularly: The PCI DSS requires a 90 day or less change cycle. By updating passwords frequently, hackers have less time to try to break the password, and you also narrow the window of time in which someone might have access to your account.

Never Share Passwords: Do not share passwords or logins with a colleague, even if you both have the same job responsibilities.

Don't Repeat Passwords: Do not use the same password for multiple systems, applications, or websites.

Strengthen Challenge Questions: Just because the question asks what your mother's maiden name is or the city grew up in, does not mean your answer has to be truthful. Come up with a consistent, but inaccurate, response that only you can easily remember.

Change Default Passwords: Default passwords for common systems and devices can be found on the Internet, making it very easy for hackers to gain access.

Limit Login Attempts: After the number of unsuccessful login attempts is reached, lock the account and require administrative assistance to unlock. The PCI DSS requires this limit be no more than six failed attempts.

REDLENS
INFOSEC