Every employee at UConn and UConn Health has a professional obligation to protect access to University systems and data, and to safeguard their log-in credentials. To protect the sensitive and confidential information that you may have access to, please carefully consider the following:

- Do NOT share your username, password or credentials with anyone for any reason.
- Do NOT allow a coworker, colleague or any other individual to access a system on your behalf using your credentials – including your supervisor or subordinates.
- Do NOT provide login credentials or personally identifiable information in response to any email.
- Do NOT write down your password or store it with corresponding account information or usernames.
- Do NOT store your password in an unencrypted file on your computer.
- Do NOT use your username as your password.
- Do NOT let anyone see you type your password.
- Do NOT sign others onto your account for their use, even if you do so without sharing your credentials.
- Passwords must be treated as confidential, protected information.
- Always remember to log off when you are no longer transacting in the system.
- Suspected security compromises or breaches related to system access/security must be reported immediately, and passwords must be changed.

Strong password security habits, such as those referenced above, not only protect access to University systems, but also help mitigate the risks of:

- Violating University and State policies
- Compromising the integrity of online approvals
- Increased data misusage
- Exposing personally identifiable information (PII) to unauthorized users.

For your reference, links to applicable University policies and resources are below:

**UCONN**

- IT Access Control Policy
- University Password Standards
- IT Acceptable Use Policy

**UCONN HEALTH**

- Systems Access Control Policy
- Acceptable Use Policy