REGULATION ON **Use of Sandburg Email and Passwords** Number 2.17.4

Carl Sandburg College email usage policy helps employees use their company email addresses appropriately. Email is essential to our everyday jobs. We want to ensure that our employees understand the limitations of using their institution email accounts. Our goal is to protect our confidential data from breaches and safeguard our reputation.

This policy applies to all administrators, faculty, staff and vendors who are assigned (or given access to) an institutional email. This email may be assigned to an individual (e.g. username@sandburg.edu) or department (e.g. dept@sandburg.edu.)

Institutional emails are powerful tools that help employees in their jobs. Employees should use their Sandburg email strictly for work-related purposes. Our employees represent the institution whenever they use their Sandburg email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

Carl Sandburg College has the right to monitor and archive all institutional emails.

Employees are allowed to use their institutional email for work-related purposes without limitations. For example, employees can use their email to:

- Communicate with current or prospective vendors, students or professional relationships.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our data.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.

- Change their email password every ninety (90) days.
- Under no circumstances share their password.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. “Watch this video, it’s amazing.”)
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they should ask Technology Services.