# PROCEDURE 2.16.3: EMAIL & PASSWORD USAGE

Email is essential to our everyday jobs, and Sandburg wants to ensure its employees understand the limitations of using their institutional email accounts.

To protect confidential data from breaches and safeguard the college's reputation, this policy applies to all administrators, faculty, staff and vendors 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).

Sandburg email is used strictly for work-related purposes, and employees represent the institution when using their Sandburg email address. Employees 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.

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

Employees can use their institutional email for work-related purposes, such as:

- Communicating with current or prospective vendors, students or professional relationships.
- Logging in to purchased software they have legitimate access to.
- Giving their email address to people for business-related networking purposes.
- Signing up for newsletters, platforms and other online services that help with 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. To help combat this, 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 90 days.
- Under no circumstances share their password.
- Avoid opening attachments and clicking on links when content isn't 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're legitimate.

- Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks, sense of urgency, etc.).

If an employee isn't sure an email received is safe, ask Technology Services.

*Original: 4/21*
*Reviewed: 1/24*
*Revised: 1/24*