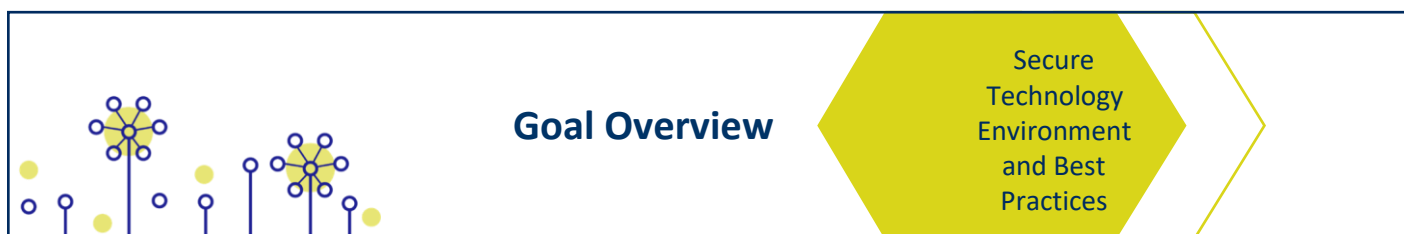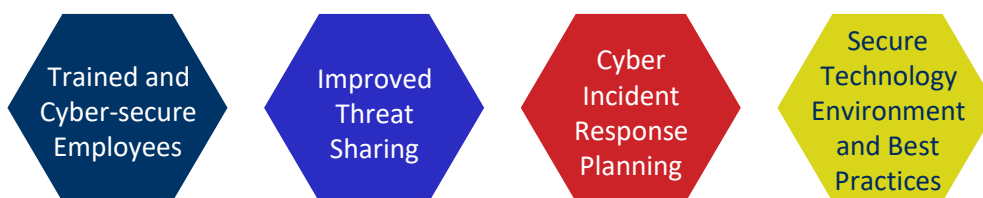# CYBER·SC

Introducing the Minimum Baseline of Cybersecurity for Municipalities—a framework for helping South Carolina municipalities improve their cybersecurity posture and protect their municipality from cyberattacks using people, process, and technology.

The purpose of defining a "minimum baseline" – the foundational level of cybersecurity municipalities should achieve – is to encourage municipalities to improve their ability to protect and defend themselves from a cyberattack, inspire collaboration, and strengthen cybersecurity resilience across SC.

The Minimum Baseline of Cybersecurity is made up of four goals:

Trained and Cyber-secure Employees   **Improved Threat Sharing**   **Cyber Incident Response Planning**   **Secure Technology Environment and Best Practices**

Goal Overview — Secure Technology Environment and Best Practices

Benefit:
Reduce the threat of cybersecurity incidents and minimize incident impacts by implementing some basic best practices to make your technology environment more secure.

How:
There are many best practices listed in the resources. Here are a few to get started:
- Application White Listing
- Require strong passwords
- Backup critical data and systems
- Update and patch systems regularly

How can creating a secure technology environment and using best practices help?
Understanding how to make your technology environment more secure involves a combination of people, process, and technology. Best practices are made up of all three layers.

1. Requiring strong passwords and putting password management controls in place means that passwords will be harder for attackers to figure out, and municipal systems will be safer.

    2. Regular backups of critical data and systems (and testing to make sure the backups work) are important in the event that there is a ransomware attack.