8 Best Practices for
Customer Data Security

Know Your Data Regulations

- Identify relevant laws (GDPR, HIPAA, CCPA, etc.)
- Track the "what," "why," and "where" of data collection
- Stay current on regulatory changes and compliance updates

Collect Only What You Need

- Limit data gathering to essential information
- Regularly audit and delete unnecessary data
- Reduce data silos by centralizing storage

Restrict and Monitor Access

- Set role-based permissions (who needs to see what)
- Use strong passwords and multi-factor authentication
- Keep a detailed record of who accesses which data

Secure Systems and Encrypt Data

- Enable encryption at rest and in transit (e.g., AES, RSA)
- Keep software and security patches up to date
- Use firewalls, antivirus tools, and secure Wi-Fi networks

Vet Vendors and Third Parties

- Check certifications (e.g., SOC 2, ISO 27001)
- Clarify data-sharing agreements and responsibilities
- Monitor vendor security practices regularly

Train Employees and Customers

- Provide regular cybersecurity training (phishing, social engineering)
- Use password managers to enforce strong password policies
- Encourage incident reporting to contain threats quickly

Back Up and Audit Regularly

- Schedule frequent, encrypted backups (store offsite copies)
- Run periodic penetration tests and vulnerability scans
- Document findings and update security policies proactively

Develop an Incident Response Plan

- Assign clear roles and responsibilities for breach scenarios
- Outline immediate steps to contain and mitigate threats
- Create a clear communication strategy (who to inform and how)

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com