Title – CRM Email Tools Policy

Policy Abstract – Birmingham-Southern College utilizes Customer Relationship Management (CRM) tools to communicate with prospects, applicants, donor prospects and active donors. The companies that host these tools send email on behalf of the College. This policy governs the onboarding and offboarding of these tools in alignment with industry standard email security practices.

Responsible Office – Information Technology, Infrastructure and Systems Support

Official – Anthony Hambey

Contact(s) – Anthony Hambey, 205-226-4849, ahambey@bsc.edu
          Rusty Howell, 205-226-3051, rhowell@bsc.edu
Applies To – All employees
Effective Date –
Revision Dates –

1. **Introduction/Background** – Official College communication is often processed through e-mail to various outside constituents via Customer Relationship Management (CRM) tools. The companies that host these tools send email on behalf of the College. Security measures must be implemented between the College's IT division and the software host companies to facilitate secure email transmission. This ensures that external threat actors are prevented from impersonating the College that could lead to theft of PII (Personally Identifiable Information).

2. **Purpose** – To ensure that proper security measures have been implemented between College technology resources and CRM partners to protect our external constituents from potential fraud.

3. **Applicable Regulations** – SACS Comprehensive Standard 12.5 – Confidentiality of Student Records and 12.7 – Physical Resources

4. **Policy Statement** –

- **Onboarding CRM Tools** – When a new CRM partner is selected, the responsible division supervisor will submit written notice to the BSC IT Helpdesk (helpdesk@bsc.edu). The notification will identify the company name, the company account manager handling the service agreement with the College, and all available contact information. BSC IT will then work with the technical team at the company so that proper security measures can be implemented. Use of the new software should not begin until these security measures have been implemented and tested. BSC IT will notify the division supervisor when these tasks have been done.
- **Changes in CRM Host Infrastructure** – Companies routinely change and upgrade host infrastructure. These changes will require BSC IT to revisit security measures in advance with the technical team of the CRM host company. Should BSC IT receive a change request, notification will be immediately provided to the supervisor of the College division that utilizes the CRM tool. Likewise, if the supervisor or user of the CRM tool receives notification of an operating change, BSC IT should be notified immediately at helpdesk@bsc.edu.
- **Offboarding CRM Tools** – When a College division makes the decision to stop using a CRM tool, notification should be given to BSC IT at helpdesk@bsc.edu. The notification should include the

end date at which time the College will no longer be using the software. BSC IT will remove all applicable security parameters connecting the College to that host company.

5. **Details** – An annual financial audit of the College contains a technology component whereby this is verified each year. Non-compliance with this policy would be reported in the form of comments in the management letter of the audit.

6. **Definitions** –

- SACS is the Southern Association of Colleges and Schools.
- CRM – Customer Relationship Management
- PII – Personally Identifiable Information

7. **References** – SACSCOC, Principles of Accreditation 2018

https://sacscoc.org/app/uploads/2019/08/2018PrinciplesOfAcreditation.pdf