Employee Records Confidentiality Policy

The company philosophy is to safeguard personal team member information in its possession to ensure the confidentiality of the information. Additionally, the company will only collect personal information that is required to pursue its business operations and to comply with government reporting and disclosure requirements. Personal information collected by the company includes team member names, addresses, telephone numbers, e-mail addresses, emergency contact information, EEO data, social security numbers, date of birth, employment eligibility data, benefits plan enrollment information, which may include dependent personal information, and school/college or certification credentials. All pre-employment inquiry information and reference checking records conducted on team members and former employee files are maintained in locked, segregated areas and are not used by the company in the course of its business operations.

Personal team member information will be considered confidential and as such will be shared only as required and with those who have a need to have access to such information. Personal information received from BMU Team Members will not be shared, sold, or conveyed to third parties for marketing or promotional purposes.

All hard copy records will be maintained in locked, secure areas with access limited to those who have a need for such access. Personal team member information used in business system applications will be safeguarded under company proprietary electronic transmission and intranet policies and security systems. Participants in company benefit plans should be aware that personal information will be shared with plan providers as required for their claims handling or record keeping needs.

Company-assigned information, which may include organizational charts, department titles and staff charts, job titles, department budgets, company coding and recording systems, telephone directories, e-mail lists, company facility or location information and addresses, is considered by the company to be proprietary company information to be used for internal purposes only. The company maintains the right to communicate and distribute such company information as it deems necessary to conduct business operations.

If a team member becomes aware of a material breach in maintaining the confidentiality of his or her personal information, the team member should report the incident it to the human resources department. The human resources department has the responsibility to investigate the incident and take corrective action. Please be aware that a standard of reasonableness will apply in these circumstances. Examples of the release of team member employee information that will not be considered a breach include the following:

• Release of partial team member birth dates, i.e., day and month is not considered confidential and will be shared with department heads who elect to recognize team members on such dates.

• Personal telephone numbers or e-mail addresses may be distributed to department head in order to facilitate company work schedules or business operations.

• Team member identifier information used in salary or budget planning, review processes and for timekeeping purposes will be shared with department heads.

•Team member's company anniversary or service recognition information will be distributed to appropriate department heads periodically.

• Team member and dependent information may be distributed in accordance with open enrollment processes for periodic benefit plan changes or periodic benefits statement updates.

BMU views the protection of personal team member information data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the company's discipline policy and may include suspension or termination in the case of severe or repeat violations. Personal team member information violations and disciplinary actions are incorporated in the company's orientation and refresher training to reinforce the company's continuing commitment to ensuring that this data is protected by the highest standards.