Ball State University Employee Confidentiality Agreement

In accordance with the trust placed in us by the University and our users, University Advancement employees are responsible for maintaining the confidentiality of the data with which they work and for keeping data secure and accessible only to those who have rights to this information. University Advancement employees routinely have access to highly sensitive information that could be considered unusual or of interest to other individuals both inside and outside of the University. Because of the sensitive nature of information accessible to personnel within University Advancement, its personnel must meet the highest standards possible for managing the University's information in a secure and professional manner.

Every employee in University Advancement is responsible for maintaining the confidentiality of data to which they may have access through privileged administrator rights. This includes protecting data from those who do not have authorization to see or access this information. No unauthorized user should see, hear or use user data without the written permission of the data owner or as authorized in writing by a senior administrator with the authority to grant access. University Advancement employees also have responsibility for securing data both while it is in use by authorized users and when it is stored or archived.

University Advancement employees may not disclose confidential information to unauthorized persons in any manner of communication, e.g. by file transfer, through written and oral communication, or other means of disclosure. University Advancement employees may not knowingly erase a data record or a data entry from any record, report or file. University Advancement employees may not remove any official record, report, file or copy of an official record or report from the office where it is maintained except in the performance of official duties.

If at any time data under the responsibility of University Advancement is thought to be compromised, either the Vice President of University Advancement or the Executive Director of University Compliance should be notified immediately. The act of intentionally disclosing user data and/or information to unauthorized persons or causing information to be compromised through gross negligence will be grounds for immediate dismissal.

I have read the above agreement and understand the condition of employment.

_____ _____

Employee Name (Printed) **Date**

_____

Employee Signature

_____ _____

Director of Advancement Services **Date**