University of Louisville

Appropriate Use Agreement
For
Third Party Vendor

Purpose

All vendors, who are granted access to data of the University of Louisville and/or its affiliated corporations (e.g. "University of Louisville Research Foundation, Inc."), ("University"), are entrusted with the maintenance of the security and confidentiality of the University's institutional systems, records and information.

Article I: Security Policies and Standards

All vendors agree to follow the University Information Security Policies and Standards in respect to systems and data access. These policies and standards are located at security.louisville.edu

Article II. Appropriate Use of Access

All vendors agree to the following Appropriate Use of Access requirements:

1. Unauthorized use or access to the University's institutional system records and information is prohibited.
2. University information will be held in strict confidence, and vendors will access and use information only for the explicit business purposes outlined in its contract with the University.
3. The University is hereby authorized and shall have the right to investigate suspected or potential abuse of its Appropriate Use Policy. If the University becomes aware of possible abuse of access, vendor access can be revoked, including all accounts, and associated passwords.
4. If system administrator rights are granted, they will apply only to the specific actions identified in this document and the vendor's contract with the University. Performance of any unrelated and/or unauthorized actions will result in the immediate termination of system administrator rights.
5. Vendor personnel must report any potential or real security instances to University personnel immediately.
6. Violation of security precautions to protect confidential information may be a crime, and may be subject to appropriate legal action and/or criminal prosecution.
7. To maintain account and password security, disclosure of any account information and passwords to anyone other than the account owner is prohibited.
8. Directly or indirectly causing the inclusion of any false, inaccurate, or misleading entries into any records or reports is prohibited.
9. Vendor must protect any accessed confidential information according to industry-accepted standards and no less rigorously than it protects its own customers´ confidential information.

10. The University must be notified immediately of any breach of confidentiality or failure to adhere or abide by these rules by the Vendor. Vendor will assume all costs associated with the breach, including notification of any and all affected users.
11. Vendor will return or securely destroy all confidential information upon completion of its contract with the University.
12. Vendor must notify the University immediately upon the termination of any system administrators connected with this contract so that account access and passwords can be revoked.
13. Vendor's system administrator is responsible for immediately removing any account access they may have set up for their employees upon termination of employment with said Vendor.

I have read and understand the rules listed above, and I agree to abide by them. I will maintain the security and confidentiality of any institutional records and information entrusted to me in the manner stated in the rules above. If there is reason to believe there is a violation of University computer security and/or state and federal laws, statutes, and regulations, I understand that my access, account(s), and account contents may become subject to monitoring and examination by authorized personnel. This agreement does not preclude any other contractual agreements that I may have with University, but a violation may render my performance in breach of such agreements.

Signature of Vendor Date

_____ _____

Printed Name and Title

Name _____

Title _____