**Determining the Risk Level of Contracts**

This guide can help you determine the risk level to UNCG when contracting for goods and services. If you have questions, please contact Risk Management for futher clarification.

|  |  |  |
| --- | --- | --- |
| **TABLE** |  |  |
| **Risk Level** | **Parameters** | **Examples** |
| High | Vendor/Supplier is authorized to use, store, access, analyze, host, etc. sensitive information/data on behalf of University (i.e. student, health, credit card, personally identifiable information)Supplier is hosting, or managing by infrastructure outside of UNCG, including in the cloud, sensitive data (i.e. student, health, credit card, personally identifiable information)Goods/services in a highly regulated industryRisk to students (safety)High risk to health and safety of university community and/or high risk to university propertyConnection to UNCG network/systems required and/orInvolving university intellectual property rights | Hosting vendors, certain SaaS, data recovery services |
| Medium | Vendor is authorized to receive, use, store, access, analyze, host, etc. sensitive information/data on behalf of University, but with University supervision (other than that above)Moderate risk to health and safety of university community and/or moderate risk to university property and/or3rd party solicitations to university community | Software implementation teams, external auditors, support providers, PR/marketing |
| Low | Vendor is authorized to access company facilities, systems, etc. which may house Sensitive Information; however, no access is granted to any Sensitive Information. | Landlords of leased facilities, janitorial services, security guards, maintenance staff, external recruiting company, etc. |
| Little/No | Vendors are not authorized to access company facilities, systems, etc. which may house Sensitive Information. | Phone company, construction/equipment company, software/hardware reseller, etc |