===== Purpose ===== The purpose of this policy is to categorize, describe, and determine the level of protection required for various types of Nested Knowledge data.

===== Scope ===== CKGE_TMP_i Nested Knowledge Data: *Company data is information generated by or for, owned by, or otherwise in Nested Knowledge's possession. Company data includes, but is not limited to, research data, business data, and computer programs. ===== III. Data Classification Policy ===== Company data refers to information generated by or for, owned by, or otherwise in Nested Knowledge's possession. Company data includes, but is not limited to, research data and business data. Data generated by independent third parties on Nested Knowledge's review platform is not under our ==== Public Data: ==== Data classified as public may be disclosed to anyone, regardless of their affiliation with Nested Knowledge. Internal Data Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of Nested Knowledge without the permission of the person or group that created the data. === Confidential === Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals, partner organizations, or Nested Knowledge. This classification also includes data that Nested Knowledge is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. === Loss of Confidentiality === Any unauthorized disclosure or loss of Confidential data must be reported to the Incident Response Team at 507-271-7051. === Restricted Use === Restricted Use data includes any information that Nested Knowledge has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require Nested Knowledge to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual. Nested Knowledge's obligations will depend on the particular data and the relevant contract or laws. The Minimum Security Standards sets a baseline for all Restricted Use data. Systems and processes protecting the following types of data need to meet that baseline: • Personally identifiable health information that is not subject to HIPAA but used in research, such as Human Subjects Data. • Personally Identifiable Information (PII), including an individual's name plus the individual's Social Security Number, driver's license number, or a financial account number. • Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens. • "Criminal Background Data" that might be collected as part of an application form or a background check. More stringent requirements exist for some types of Restricted Use data.*