# Exhibit C – Institutional Information

This exhibit describes the Institutional Information for the benefit of both parties.

#### Protection Level Classification[5](#_bookmark4):

|  |  |
| --- | --- |
| **Protection Levels Needed** | **Anticipated Record Count** |
|  Protection Level 1 |  |
|  Protection Level 2 |  |
|  Protection Level 3 | * Less than 70,000 * More than 70,000 |
| X Protection Level 4 | Less than 70,000  X More than 70,000 |

**Explanation**:

The Protection Level and anticipated record count determines the applicable cyber security insurance requirement in the Terms and Conditions.

#### Institutional Information data element descriptors:

Select all data types that apply:

* 1.  Animal Research Data.
  2.  Controlled Technical Information (CTI).
  3.  Controlled Unclassified Information (CUI) – 800-171/NARA.
  4.  Defense Department: Covered Defense Information (CDI).
  5.  Federal Acquisition Regulations (FARS/DFAR) other than CUI.
  6.  European Privacy Law (EEA and UK GDPR) personal data.
  7.  European Privacy Law (EEA and UK GDPR) special data.
  8. x Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
  9. x Health Records subject to HIPAA Privacy or Security Rule (PHI).
  10.  Human Subject Research Data.
      1.  Identified.
      2.  Anonymized.
  11.  Intellectual property (IP), such as patents, copyright, or trade secrets.
  12.  ITAR/EAR-controlled data.

5 For more information about classification see: https://security.ucop.edu/policies/institutional-information-and-it- resource-classification.html.

* 1.  Payment card data (PCI, PCI DSS).
  2.  Personally identifiable information – PII.
  3.  Student data, whether or not subject to FERPA.
  4.  Other:
  5.  Other:

#### Regulation or Contracts Relating to the Institutional Information:

Select all regulations or external obligations that apply to inform UC and the Supplier of obligations related to this Appendix:

##### Privacy (\* indicates data security requirements are also present)

* 1. x California Confidentiality of Medical Information Act (CMIA) \*.
  2. x California Consumer Privacy Act (CCPA).
  3. x California Information Practices Act (IPA).
  4.  European Privacy Laws Regulation (EEA and UK GDPR)\*.
  5.  Family Educational Rights and Privacy Act (FERPA) \*.
  6.  Federal Policy for the Protection of Human Subjects (“Common Rule”).
  7.  Genetic Information Nondiscrimination Act (GINA).
  8.  Gramm-Leach-Bliley Act (GLBA) (Student Financial Aid) \*.
  9. x Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) \*.
  10.  Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2).
  11.  The Fair and Accurate Credit Transaction Act (FACTA).
  12.  The Fair Credit Reporting Act (FCRA).

Data Security

* 1.  Chemical Facility Anti-Terrorism Standards (CFATS).
  2.  Defense Federal Acquisition Regulations (DFARS).
  3.  Export Administration Regulations (EAR).
  4.  Federal Acquisition Regulations (FARS).
  5.  Federal Information Security Modernization Act (FISMA).
  6.  International Traffic in Arms Regulations (ITAR).
  7.  Payment card data (PCI, PCI DSS).
  8.  Toxic Substances Control Act (TSCA).
  9.  Other:

# 

# Exhibit D

Supplier’s I

Initial Information Security Plan