

## Data Classification and Handling Policy

### APPENDIX 1: Data Classification Levels I, II and III

- ◆ **Level I – Confidential Information:** High risk of significant financial loss, legal liability, public distrust or harm if this data is disclosed.

Examples include:

- Data protected by HIPAA (health information)
- Data protected by FERPA (student information including grades, exams, rosters, official correspondence, financial aid, scholarship records, etc.)
- Data protected by GLB (financial information)
- Data subject to PCI (credit or payment card industry) standards
- Data subject to other Federal or state confidentiality laws
- Donor or prospect information
- Passwords and PINs
- Personally Identifiable Information (“PII”)
- Personnel data
- Individually identifiable information created and collected by research projects
- Certain research data with National Security implications
- Data subject to protection pursuant to non-disclosure agreements
- Audit working papers
- Data protected by attorney/client privilege
- Email covering topics listed above

- ◆ **Level II – Sensitive Information:** Moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, public distrust, or harm if this data is disclosed.

Examples include:

- Audit reports
- Email addresses that are not a public record
- Other grants and contracts (not included above)
- Competitive business information
- System security information such as firewall rules and hardening procedures
- Security incident information

- ◆ **Level III – Public Information:** Low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust or harm if this data is disclosed.

Examples include:

- University directory information, as defined by the Student Records Policy (<https://policy.drupal.ku.edu/registrar/student-record-policy>)
- Blogs
- Web pages
- Course offerings
- Annual reports, etc.