ECU Classification Levels *

**Level 1—Public**

*Public data includes, but is not limited to: Advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases.*

• University data that is purposefully made available to the public.
• Disclosure of Level 1 data requires no authorization and may be freely disseminated without potential harm to the university.

**Level 2 – Internal**

*Internal data includes, but is not limited to: Budget and salary information, personal cell phone numbers, departmental standard operating practices, internal memos, incomplete or unpublished research. While some forms of internal data can be made available to the public, the data is not freely disseminated without appropriate authorization.*

• University owned or managed data that includes information that is not openly shared with the general public but is not specifically required to be protected by statute or regulation.
• Unauthorized disclosure would not result in direct financial loss or any legal, contractual, or regulatory violations, but might otherwise adversely impact the university, individuals, or affiliates.
• Level 2 data is intended for use by a designated workgroup, department, or group of individuals within the university.

**Level 3 - Confidential/Sensitive**

*Confidential/sensitive data includes, but is not limited to: Passport data, certain research data (e.g., proprietary or otherwise protected) and Student data that is not designated as directory information.*

• University owned or managed data that is confidential business or personal information for which unauthorized disclosure could have a serious adverse impact on the university, individuals or affiliates.
• Level 3 data is intended for a very specific use and should not be disclosed except to those who have explicit authorization to review such data.
• There are often general statutory, regulatory or contractual requirements that require protection of the data.
• Data whose loss, corruption, or unauthorized disclosure would constitute a violation of Federal, State and/or International laws. Some examples include data deemed confidential in contract agreements, Family Educational Rights and Privacy Act (FERPA), State Human Resources Act (SHRA), Graham-Leach-Bliley Act (GLBA), NCGS 125-18 (Library Records: Definitions), NCGS 125-19 (Library Records: Confidentiality of library user records) and General Data Protection Regulation (GDPR).

**Level 4 - Highly Restricted**

*Highly restricted data includes, but is not limited to: Social Security Numbers, payment card numbers, medical records, and restricted information protected by nondisclosure agreements, restricted research data.*

• University owned or managed data that is highly restricted business or personal information, for which unauthorized disclosure would result in significant financial loss to the university, impair its ability to conduct business, or result in a violation of contractual agreements.
• Level 4 data is intended for very limited use and must not be disclosed except to those who have explicit authorization to view or use the data.
• There are often governing statutes, regulations, standards, or agreements with specific provisions that dictate how this type of data must be protected.
• Data with a known protection or disclosure standard whose release to an unauthorized person would be a violation of Federal, State and/or International laws. Some examples include data covered by Health Insurance Portability and Accountability Act (HIPAA), The Federal Information Security Management Act (FISMA), the North Carolina Identity Theft Protection Act, NCGS 143-748 (Internal Auditing: Confidentiality of internal audit work papers), and data covered by Payment Card Industry (PCI) compliance requirements.

* Combinations or subsets of data may need to be classified at a higher level of security. In addition, Data elements that are shared or traverse multiple systems may require that the most restrictive protections be applied to the data.

Last Update: 11/13/2018